User Manual

© TSSI 2001

Document Reference: OM/207/02

For *Verid*+ Firmware version VP5.01

18th February 2002

TSSI Contact Details

TSSI Technical support:	Tel: +44 1793 747747	Fax: +44 1793 747701
TSSI Reception:	Tel: +44 1793 747700	Fax: +44 1793 747701
e-mail:	*Verid*@tssi.co.uk	
web	www.tssi.co.uk	

Limited Warranty and Disclaimer of Liability

Thorn Secure Science Ltd. warrant that the *Verid+* unit will be free from defects in materials and workmanship under normal use and service during the first twelve months from the date of purchase. The *Verid+* unit and the information in this manual are provided "as is". Thorn Secure Science Ltd. makes no other representations or warranties express or implied with respect to the *Verid+* unit or the written manual, including their quality, performance, merchantability or fitness for a particular purpose. Thorn Secure Science Ltd. does not warrant, guarantee, or make any representations regarding the use, or the results of the use of the written manual in terms of correctness, accuracy, reliability, currentness, or otherwise. The entire risk, as to the results and performance of the unit, is assumed by you.

In no event will Thorn Secure Science Ltd. or its suppliers be liable for any damages whatsoever (including, but not limited to damages for loss of business profits, business interruption, loss of business information, loss of data, claims by third parties, incidental or consequential damages or any other pecuniary loss) arising out of the use or inability to use the unit or the written manual, even if Thorn Secure Science Ltd. or an authorised Thorn Secure Science Ltd representative has been advised of the possibility of such damage. In any case Thorn Secure Science Ltd's entire liability shall be the repair or replacement or a refund of the *Verid+* unit or written materials, at Thorn Secure Science Ltd's option, which are returned to Thorn Secure Science Ltd during the first ninety (90) days from the date of purchase or delivery and which breached a specific warranty hereunder. The warranty and remedies are exclusive and in lieu of all others, oral, written, expressed or implied. No Thorn Secure Science Ltd distributor, agent or employee is authorised to make any modifications or additions to these terms.

Due to continual product development, TSSI reserves the right to change the product specification and manuals without notice.

Copyright

© TSSI 2002

Trade Marks

TM - *Verid+* and Watermark are trademarks of TSSI. All other trademarks are recognised.

Contents:

1 Getting started quickly – how to avoid reading the manual! 5

2 General Introduction 6

3 Receiving a new unit 6

3.1 Factory default settings 6
3.2 Enrolment and Verification – key differences 7
3.3 Identifying your Verid+ 7

4 Installation details 7

4.1 Fixing to the wall 8
4.2 Connecting power 9
4.3 Connecting a PIN device 9
4.4 Checking the PIN device works 13
4.5 External control of the PASS (unlock) and FAIL (locked) LEDs on Verid+. 14
4.6 Using the TimeOut and CardPresent signals. 14
4.7 Connecting Verid+ to the Access Control system. 14
4.8 Error codes output by Verid+ 16
4.9 Terminal block connections and pin-outs. 17

5 Changing the way the unit is configured (Verid Manager) 17

5.1 General principles – SuperUsers, Supervisor and Configuration 17
5.2 SuperUser 18
5.3 Supervisor – option commands 18
5.4 Configuration – option commands 19
5.5 LCD text – changing the displayed messages 20

6 Using the unit for the first time 21

6.1 Important concept – “Users” and “SuperUsers” 21
6.2 Important concept – “Security Levels” 21
6.3 Tips when using biometric systems 22
6.4 Enrolling the first SuperUser 23
6.5 Enrolling all other people 24

7 Adding and Deleting users – Template Database Management 26

7.1 Overview - Template transfer 26
7.2 Adding and deleting templates via the RS232 port 26
7.3 Emptying the database – Verid Manager 27
7.4 Managing the database – Verid Manager 27

8 Guidelines - Networking Verid+ units. 28

8.1 Installing (wiring) a Verid+ network 28
8.2 Setting up a *Verid+* network without reading the manual. 29
8.3 Verid+ Network – power up LED sequencing 30
8.4 Verid+ Network – auto-configure 32
8.5 Installing a simple Verid+ network 32

8.6 Verid+ network – Adding additional units 33
8.7 Technical guidelines for installing an RS485 network 33
8.8 Using Verid Manager with networked units 33

9 Storing templates on magnetic cards 35

9.1 Using templates on a magnetic card: 35
9.2 Generating and verifying track 3 templates using Verid+ 35
9.3 Encoding templates onto track 3 36

10 Fault finding / Troubleshooting / Safety 37

10.1 Troubleshooting & frequently asked questions 37
10.2 Maintenance / spares / replacement parts 38
10.3 Compatibility with earlier versions of Verid. 39

11 A technical overview 40

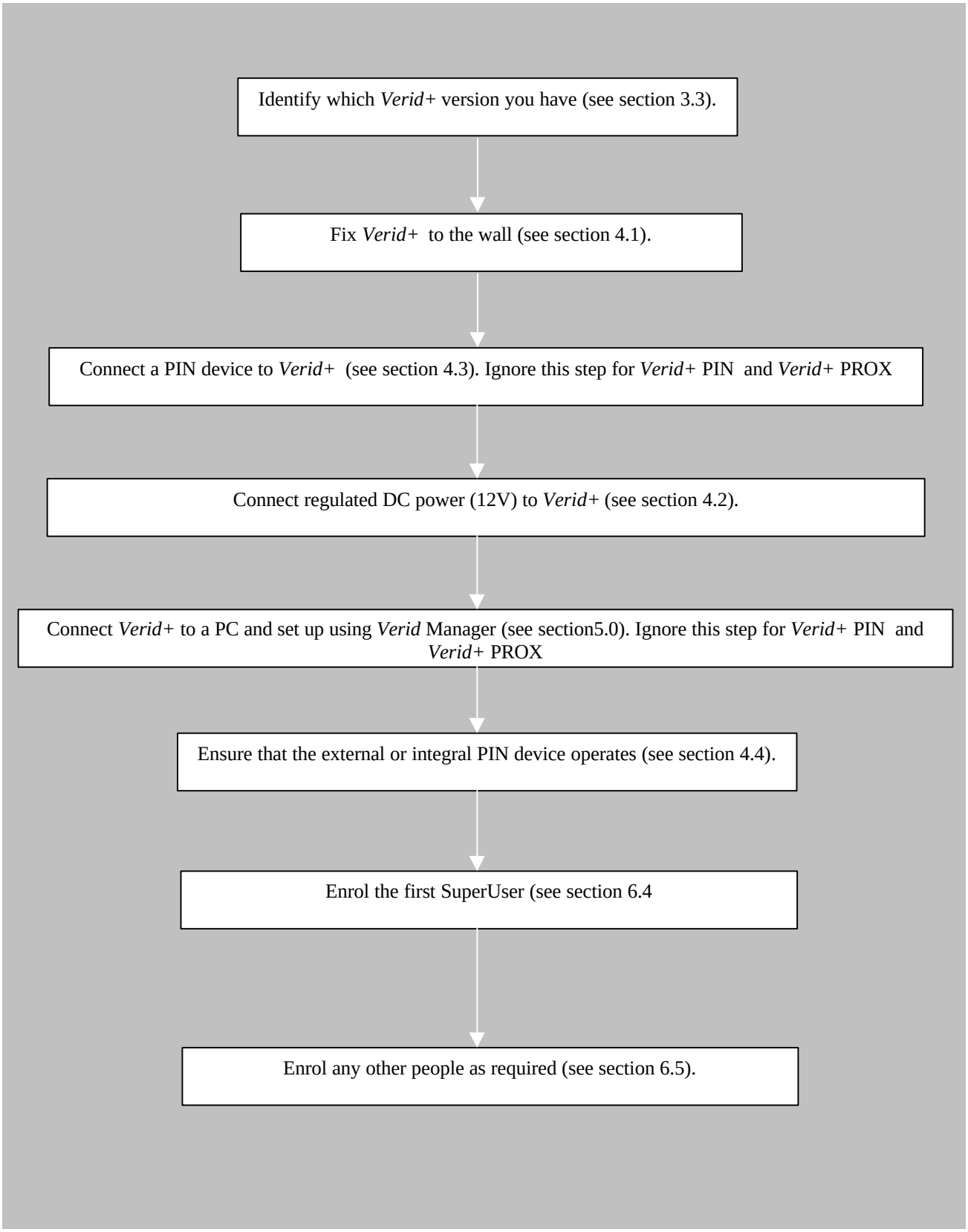
11.1 Fingerprint matching algorithm 40
11.2 Maximum number of users 40
11.3 Special Features 40
11.4 TTL signal timing diagrams 41
11.5 Cable connecting Verid+ to a PC 43
11.6 Glossary 44

12 Specification 45

12.1 Applicability (document versions) 46
12.2 Changes to this manual 46

13 Index 47

1 Getting started quickly – how to avoid reading the manual!


Identify which *Verid*+ version you have (see section 3.3).
Fix *Verid*+ to the wall (see section 4.1).
Connect a PIN device to *Verid*+ (see section 4.3). Ignore this step for *Verid*+ PIN and *Verid*+ PROX
Connect regulated DC power (12V) to *Verid*+ (see section 4.2).
Connect *Verid*+ to a PC and set up using *Verid* Manager (see section5.0). Ignore this step for *Verid*+ PIN and *Verid*+ PROX
Ensure that the external or integral PIN device operates (see section 4.4).
Enrol the first SuperUser (see section 6.4
Enrol any other people as required (see section 6.5).

2 General Introduction

The *Verid+* fingerprint verification units are truly standalone devices, designed to provide access control systems with instant improved security, or to act as a means of identity verification in a wide range of different applications.

The Verid+ fingerprint verification units are available as 3 variants:

Verid+ is a stand-alone unit that can be added to existing access control systems and readers, it contains no PIN entry device. Verid+ is designed to work with Magnetic Card readers, Proximity readers and Wiegand keypads.

Verid+PIN contains an integrated PIN pad, no additional PIN entry device is needed.

Verid+PROX is fitted with an integrated Proximity reader, which operates with HID compatible cards.

When used in an access control system *Verid+* is installed between the existing PIN device and door controller, and confirms the identity of the person. In most cases installation requires no changes to the existing PIN devices, cards or access control system.

The complete fingerprint verification process and fingerprint database storage is performed within the single wall mounted housing, which also contains terminal block connectors on a back plate for easy installation.

Installation of fingerprint verification is quick and easy with TSSI's *Verid+* system. *Verid+* supports many types of PIN entry devices - and emulates them for easy integration into existing systems. No system software changes are needed and users can be enrolled with their normal access control cards. *Verid+*'s "plug and play" approach provides instant additional security and a card holder's identity can be verified in under 1 second. For convenience and practicality, each person can enrol with one or two fingers.

3 Receiving a new unit

Verid+ supports many different PIN device technologies and can be integrated into an existing access control system in a variety of ways. Many of *Verid+*'s features can be enabled if and when they are needed, but before installation, it is important to check the factory default settings against the installation requirements.

3.1 Factory default settings

The following are the factory defaults for new *Verid+* units.

Feature	Factory default settings	Alternative configurations	To change, see section…
PIN device Input and Output ***Verid+ only***	General Wiegand	OMRON /MAGTEK/ Watermark / Proximity, ISO track 2.	Section 4.3
PIN device Input and Output ***Verid+PIN only***	Input:Not applicable Output: Track 2	Not applicable	Not applicable
PIN device Input and Output ***Verid+PROX only***	Input:Not applicable Output: Wiegand 2601	Not applicable	Not applicable
Card Present ***All Verid+ types***	Not required for input and so not enabled as output.	Can enable use as both input and output.	Section 4.6
Time Out Present ***All Verid+ types***	Not required for input and so not enabled as output.	Can enable use as both input and output.	Section 4.6

Lock/Unlock ***All Verid+ types***	Will illuminate GREEN or flashing RED if fingerprint matches or fails respectively.	Can be externally controlled by two logic line inputs.	Section 4.5
Storage of fingerprint templates. ***All Verid+ types***	All templates and associated PINs are stored in non-volatile memory inside *Verid+*.	Track 3 of a magnetic stripe card. (Additional equipment needed contact TSSI for details.)	Section 9.
LCD text ***All Verid+ types***	English language	Configurable to single or double byte character sets.	Section 5.5. Some languages are available from TSSI.
Security level ***All Verid+ types***	Set at level 3	Levels 1 to 5	Section 6.2.1

Table 1 : Factory default settings

3.2 Enrolment and Verification – key differences

All *Verid+* units can perform both Enrolment and Verification. Enrolment is the process of registering new users on the system and is normally only necessary once. Verification is the process of checking that an enrolled user is the correct person.

3.3 Identifying your Verid+

To use this manual correctly you need to know which *Verid+* variant you have. Each is packed with an installation card, which states which *Verid+* variant has been supplied. In addition the images below will help you identify the variant.

Figure 1: Verid +

Figure 1 : *Verid+PIN*

Figure 3 : *Verid+Prox*

4 Installation details

Every new *Verid+* unit is supplied ready to install. Each is supplied with an installation card which is specific to the *Verid+* variant. Units are supplied without any users in the internal database. The following items can be supplied:

- Any updates to this manual – the most recent manual is available to customers on www.tssi.co.uk.
- *Verid Manager* software (Windows ’95 or ’98), manual and RS232 cable to connect a PC to *Verid+*.

4.1 Fixing to the wall

Verid+ units are designed to be wall mounted, but can operate on a desktop. *Verid+* units should be installed:

a) Indoors, out of direct sunlight. (*Verid+* has not been designed for outdoor use)

b) In an upright position, on a flat wall robust enough to support *Verid+*.

c) At a suitable height for all users, usually between 1m and 1.4m above floor level

d) Conveniently close to the existing access control PIN device.

e) In a position where a person can comfortably use the unit with a finger from left or right hand resting on the *Verid+* sensor. For safety this position should not put the user at risk of being hit if the door is suddenly opened from inside the protected area.

f) At least 75mm away from any side wall.

Once a suitable position has been found, fix the unit flush against the wall as follows, and see Figure 4, below:

NOTE - Allow 8mm clearance around the sides and top of the back plate (shown below) for fitting the front cover. Leave adequate clearance below the unit so that the screws securing *Verid+* to the back plate can be tightened at the end of the installation.

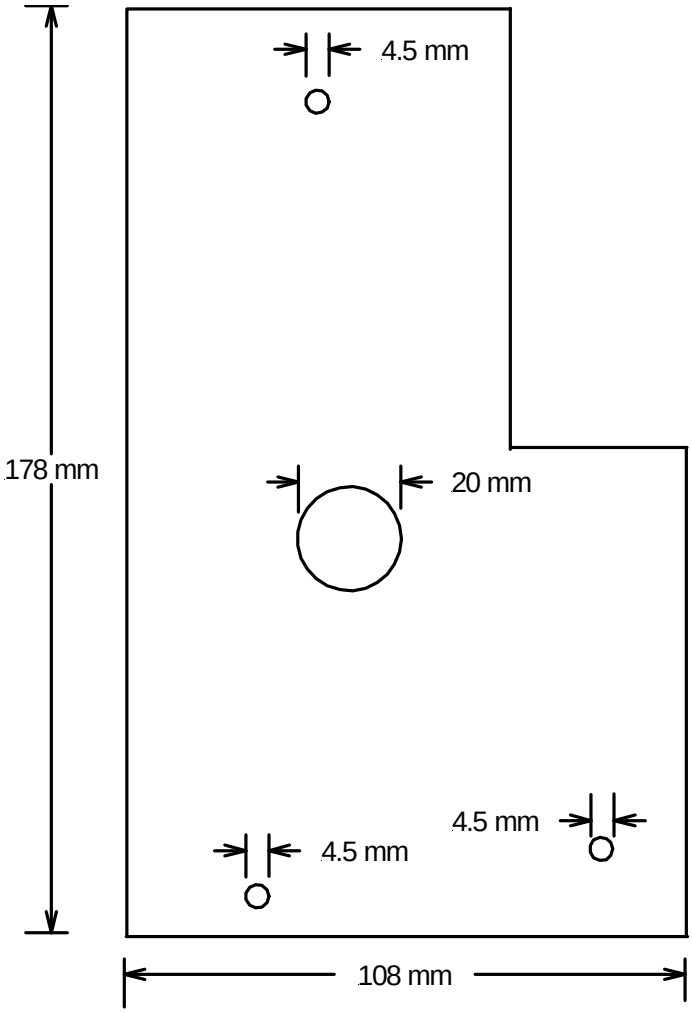


Figure 4 : Back plate showing mounting hole positions.

a) Using the back plate as a guide, mark the centre position of the three fixing holes ensuring the unit is level and square.

b) Drill three 6mm holes and insert suitable wall plugs

c) Locate the back plate in position and secure to wall with four No.10 dome head screws and wall plugs (not supplied).

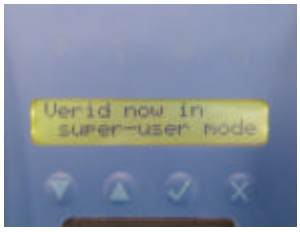
d) Connect the PIN device and access control system to the terminals on the connector block. Then connect the ribbon cable from the *Verid+* unit to the back-plate.

e) Insert the top of the housing over the back plate and fasten using the two bolts on the base of the unit. For maximum security we recommend the use of anti-tamper bolts (size M4) - not fitted as standard.

4.2 Connecting power

Power is connected to the 0V and +12V terminals on J2. The input voltage should be in the range +10V to +14V and current consumption (of *Verid+* only) is approx. 250mA. Use a power supply capable of delivering 500 mA to ensure trouble free operation.

The *Verid+* unit can supply 5V and 12V to an external PIN device (see section 4.9). The maximum current available (on the 5V supply) to drive external devices is 100 mA. The maximum 12V output current is only limited by the power supply used - check the power supply used has adequate capacity. In order to meet the safety requirements of EN60950 *Verid+* should be powered from an SELV supply.



When the unit is powered up *Verid+* will initially cycle through a self test sequence to determine the network and configuration status. This is described in section 8.3. Once this test is complete the display will indicate that *Verid+* is in Super-User mode.

Figure 5: Power applied to *Verid+*

4.3 Connecting a PIN device

Verid+ has been designed to support PIN entry from a variety of devices – track 2 card readers, proximity readers, keypads with Wiegand or track 2 outputs, Watermark and Wiegand readers. Directions for connecting each type of reader, and details of the compatible card formats, are given in the following sections. All new *Verid+* units are delivered to accept input from a Wiegand input device. The default setting of "0 bits" allows readers with various bit lengths to be used. However within a system all readers should output the same bit length. NOTE: when set at "0 bits" *Verid+* cannot decode the PIN number, it merely stores it and re-transmits it after a successful verification. In this case *Verid+* generates an internal template reference for the PIN number.(See section 3.4.4). Changing the reader to accept signals from other devices can be accomplished with *Verid Manager* or the RS232 commands - see TSSI document OM205.

4.3.1 Connecting a track 2 reader

To connect a track 2 reader to *Verid+*, wire the clock and data lines from the reader into the appropriate clock and data terminals in *Verid+* (terminals **Clock 1** and **Data 1** in J7), (see Section 4.9 on page 17). Figure 6 below shows the connections for a MAGTEK reader and Figure 6a for an OMRON standard reader. Both these are shown powered from the auxiliary power output from *Verid+*. To change the card input device from MAGTEK to OMRON requires the unit to be re-configured, either using *Verid Manager* (see TSSI document OM201) or the RS232 command (see see TSSI document OM205).

N.B. For convenience, *Verid+* has been factory set **not** to require either "TimeOut or "CardPresent" signals. Either or both or these can be enabled (see section 4.6).

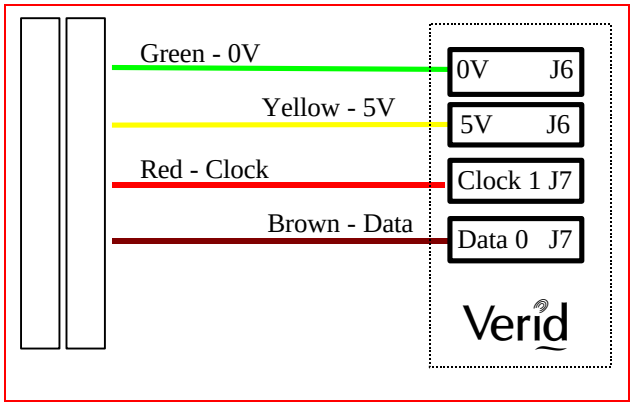


Figure 6 : Connecting a MAGTEK MT2105002 reader

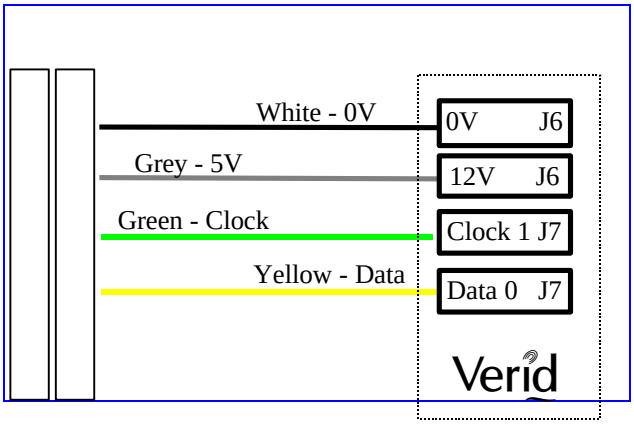


Figure 6a : Connecting an OMRON reader

4.3.1.1 Track 2 swipe reader - Compatible card formats

When configured for track 2 PIN entry, the *Verid+* unit will be able to decode all ISO 7811/2 track 2 compatible cards. The maximum PIN length is 16 digits (excluding ISO start, end sentinels and LRC characters). Contact TSSI if planning to use PINs with more than 16 characters.

4.3.2 Connecting a Wiegand swipe reader

A Wiegand swipe reader must be connected using the "0" and "1" data lines on J7 (See section 4.9)

N.B. Because of the number of different Wiegand data formats, only some Wiegand PIN device formats are supported by *Verid+*. This section relates *only* to card readers which do not in any way "interpret" the Wiegand data. "Intelligent" card readers (e.g. certain types of proximity) that process card data and then output in "Wiegand format" are dealt with in section 4.3.4. An "intelligent" reader is one that always outputs a card data with the same bit pattern, in the same direction, every time the card is presented.

4.3.2.1 Wiegand swipe reader - Compatible card formats

For unintelligent Wiegand card readers that do not interpret card data, the card data must conform to the Wiegand 2601 standard (see Table 2 below).

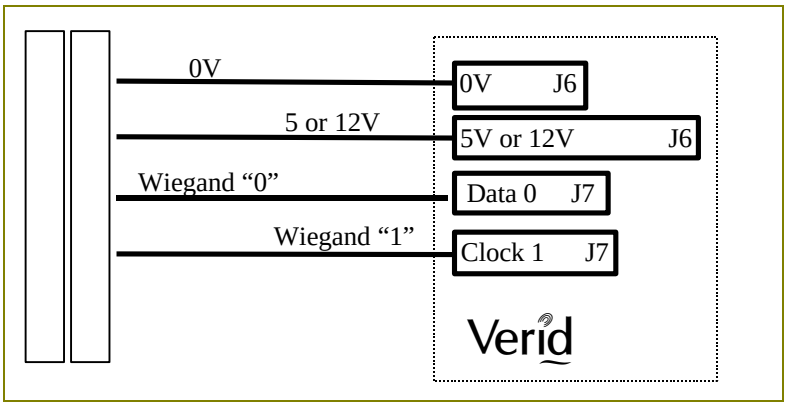


Figure 2 : Connecting a Wiegand reader.

Wiegand "2601" data received and transmitted by *Verid+* shall consist of 26 bits – the first and last bit are parity bits, with the central 24 bits being data as shown below:

Bit #		0	1	2
		123456789	0123456789	0123456
Data:		PXXXXXXXX	XXXXXXXXXX	XXXXXXP
Parity:		PEEEEEEEE	EEEE	
			000000	000000P

Table 2 : Data format - Wiegand 2601

P- Parity is checked by summing the binary value "1" data bits in a parity field. The field of bits #1 to #13 (inclusive) should sum to be an even (E) count. The field of bits #14 to #26 (inclusive) will sum to be an odd (O) count.

4.3.3 Connecting a Proximity reader to the unit

Proximity readers can be connected to *Verid+* provided they can emulate either a "ISO track 2" card data output, Wiegand 2601 output or an "Intelligent Wiegand reader". In all cases the card data must conform to the relevant card data formats. *Verid+* will need to be configured to expect the appropriate PIN input device and appropriate data signal connections must be made, (see section 4.9).

4.3.4 Connecting an "intelligent" Wiegand card reader to the unit

Many readers (e.g. proximity readers) have the ability to output card data in a "Wiegand" format. For the purposes of connecting to *Verid+*, a reader is "intelligent", if it **always** outputs the **same** (Wiegand) bit pattern, in the **same** direction, **every** time the card is presented (regardless of the speed or direction of card movement).

In this mode, *Verid+* will (internally) store templates against a pseudo-PIN that it has generated internally. The pseudo-PIN is unique, but may have no obvious relationship with the PIN as reported by the host access control system. (This is because *Verid+* has no knowledge of the data format etc. of the incoming data).

4.3.4.1 Compatible "intelligent" Wiegand formats

If the reader output is "intelligent Wiegand", the only constraint is that the total number of bits on the "pseudo" Wiegand card be less than or equal to 64 bits. In this mode, *Verid+* will not interpret the data and therefore requires no knowledge of the data format. *However, the consequence of this is that Verid+ does not perform any checks on the integrity of the data, its content or format. It is assumed the "intelligent" reader will have made these checks.* When the "intelligent" reader has a Wiegand output, the "0" and "1" lines should be connected to the terminals in J7.

Using *Verid* Manager, *Verid+* can be configured to "extract" a PIN number from the input Wiegand bit stream. There are four ways of configuring *Verid+* when dealing with "intelligent" readers:

1. "ignore leading zeros", i.e. PIN number is derived using whatever is left from the incoming data, once all leading zeros are stripped from the data.
2. "take bit pattern exactly as received", i.e. PIN number is derived using every single incoming bit.
3. "use exactly "n" bits of incoming data", no incoming bits are stripped or ignored and exactly "n" bits are used as the PIN. The maximum number of bits is 64.
4. "ignore leading zeros and then use the next "n" bits as the PIN" , i.e. this is a combination of other cases as explained above.

The table below illustrates how each option affects what *Verid+* uses as the PIN.

Bit pattern from PIN device.	0000 0000 0110 0111 0000 0000 1010 0001 1010 0010 0000 0000 00
Verid+ Configuration.	Bit pattern used by *Verid+* as PIN.
Ignore leading zeros	110 0111 0000 0000 1010 0001 1010 0010 0000 0000 00
Take bit pattern exactly	0000 0000 0110 0111 0000 0000 1010 0001 1010 0010 0000 0000 00
Bit length is 36 bits	0000 0000 0110 0111 0000 0000 1010 0001 1010
Ignore leading zeros and bit length is exactly 26 bits	110 0111 0000 0000 1010 0001 101

Table 3 : "Intelligent" Wiegand settings

4.3.4.2 Changes to Wiegand 2601 decoding

In VP5.01 the way in which the Weigand 2601 decoding works has been changed. This has been improved for better de-coding of both Site Code and User number (which is 8 digits). These changes mean that VP5.01 Verid + units are no longer compatible with previous versions – ***if the Weigand 2601 setting is in use on these previous versions.***

4.3.5 Connecting a Watermark 130x series reader to the unit.

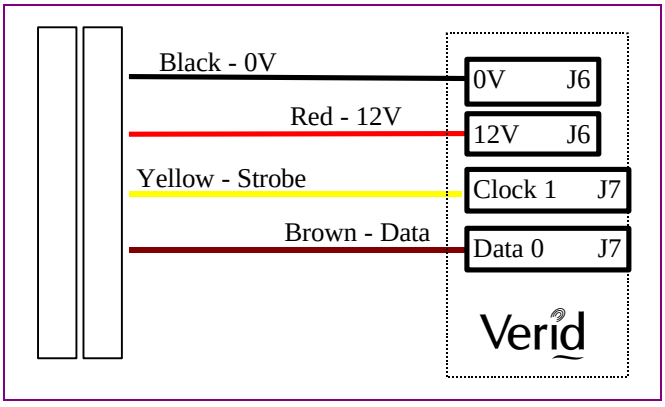


Figure 3 : Connecting a 130x Watermark reader

4.3.5.1 Compatible Watermark card formats

Verid+ supports all registered Watermark formats.

4.3.6 Connecting a 4 by 4 keypad to the unit

The connection of an external 4 by 4 row and column Keypad to *Verid+* is not possible. Only keypads with track 2 or Wiegand outputs can be connected. If a keypad is required the use of *Verid+* PIN with its integral keypad is recommended.

4.3.6.1 Compatible PIN formats

The factory default for length of PIN input from a keypad is 4 digits. This can be changed to any number between 1 and 16 – and can be changed using *Verid Manager* (see TSSI document OM205).

N.B. The PIN number is output to the door controller as ISO track 2 data, in either OMRON or MAGTEK timings, therefore "B" and "F" are ***not*** allowed as PIN characters.

4.3.7 Connecting other reader types

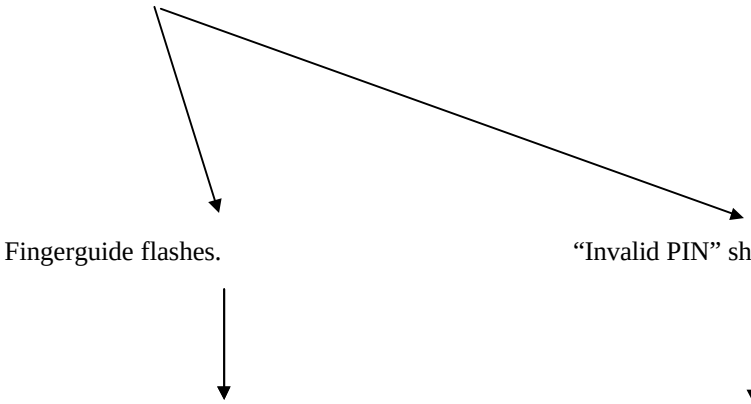
Reader types other than those mentioned above can be connected to *Verid+* if they communicate using one of the interface formats supported by *Verid+*. If your preferred reader type is not listed then contact your local distributor or TSSI before commissioning a system. In some cases a reader with an interface not supported by *Verid+* may be settable to a usable format such as Wiegand or Track 2, in this case select that interface on both Verid+ and the reader.

4.4 Checking the PIN device works

Once power and the PIN device are connected, and the *Verid+* unit configured, the PIN number should be correctly decoded. This can be tested as follows:

- Ensure that the reader and *Verid+* are powered up.
- Ensure that *Verid+* has an empty database and automatically enters SuperUser mode on power-up.
- Ensure that the PIN device connections are correct and that the PIN device is the type expected by *Verid+*.

  N.B. It is not necessary for the Door Controller to be connected at this stage.
- Power-up the unit ensuring that it enters SuperUser mode, select "Add a new user" as described in section 6.4. Swipe a card through the reader or enter a PIN.



Fingerguide flashes.

Verid+ has successfully decoded the card data.

"Invalid PIN" shown on LCD display

Either the card has not been swiped correctly or *Verid+* has not understood the card format or data signals. Re-swipe the card a couple of times to ensure the swipe action has not caused the fault. Then check the wiring and configuration settings, and TTL signal requirements (see section 11.4) against those from the PIN device.

4.5 External control of the PASS (unlock) and FAIL (locked) LEDs on Verid+.

The PASS (unlock symbol) and FAIL (locked symbol) LEDs on *Verid+* are factory set to be internally controlled and will illuminate GREEN or flash RED upon the success or failure of a fingerprint match.

Using *Verid Manager* or an RS232 command, (see TSSI document OM205), these LEDs can be externally controlled by the two inputs on J4 driven by 5V logic levels. Ensure that the terminal "0V" on J4, is connected to the 0V of the device controlling the input lines connected to terminals "PASS LED", and "FAIL LED . These are 'active low' high impedance input with 100kΩ pull up resistors.Taking an input low activates the corresponding LED.

Pass LED	Fail LED	Result
1	1	No action
0	1	Green unlock symbol
1	0	Red lock symbol
0	0	Invalid (both symbols)

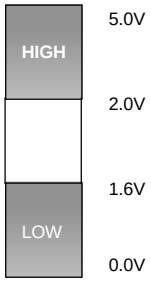


Table 4 : External LED control

4.6 Using the TimeOut and CardPresent signals.

In the factory default condition, neither TimeOut nor CardPresent signals are required for PIN input, and importantly, neither line is output by *Verid+*.

If the door controller or access control system requires either or both of these lines, they can be turned on using *Verid Manager* or implementing an RS232 command (see document OM205). The timing diagram in section 11.4 gives details of these signals.

N.B. *Verid+* will not output the TimeOut or CardPresent lines unless configured to do so.

4.7 Connecting Verid+ to the Access Control system.

Once a finger has been successfully verified, the PIN number is forwarded to the access control system (or door controller). With the exception of a PIN pad, the data is output in the same format as it is received from the PIN entry device. PIN pad data is output in ISO track 2 format with either MAGTEK or OMRON timings. PIN data is only sent from *Verid+* after a successful template match has occurred.

The "CardPresent" and "TimeOut" signals are also output from *Verid+* if they have been enabled and correctly received. **Note: All connections to the access control system are located on terminal block J3.**

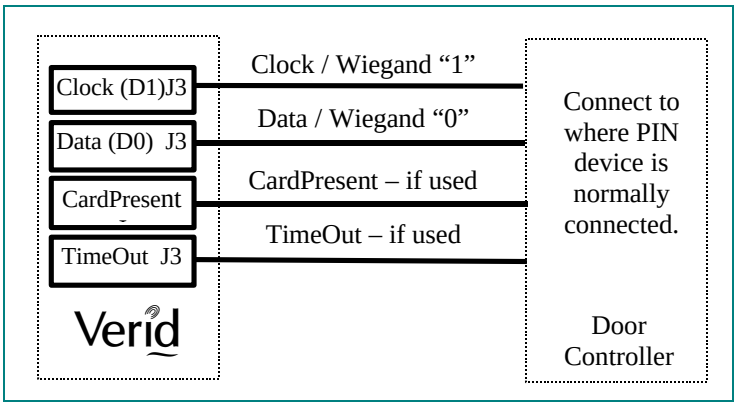


Figure 4 : Connections to the door controller

4.7.1 Connecting *Verid+* to a local door relay

As an alternative to connection to an Access Control System *Verid+* can control the solenoid of a local, electrically operated door lock. A door relay driver is fitted as standard. Be aware that this way of operating a door is a lower security option.

The function of the door relay driver is to switch the solenoid of a local, electrically operated door lock. A separate power supply is required to run the door lock. Where possible the input to this power supply should be taken from a different point to that used for the *Verid+* power supply. Electrically operated door locks produce large transient voltage spikes, *Verid+* may be affected if these spikes couple to the *Verid+* inputs.

As standard, *Verid+* units running VP1.00 firmware and later are already configured to control a door relay driver, so no changes to firmware settings should be needed.

The connections for the door relay driver are located on terminal block J5. When *Verid+* matches a finger the relay will be energised to open the door lock. If necessary an over-ride switch can be fitted as well.

Note:The door lock must be of the 'ENERGISE to UNLOCK' type, rated at no more than 12V DC, 500mA, if the lock power requirement exceeds this you MUST use Verid to switch a suitably rated relay.

Door Lock	***Verid+* Connections**
Terminal 1 0 V door lock supply	N0 Doorlock terminal 2
Terminal 2 N.O. Contact	Common 12 Volts door lock supply

Over-ride Switch

Common	12 Volts door lock supply
N/0	Verid+ J5

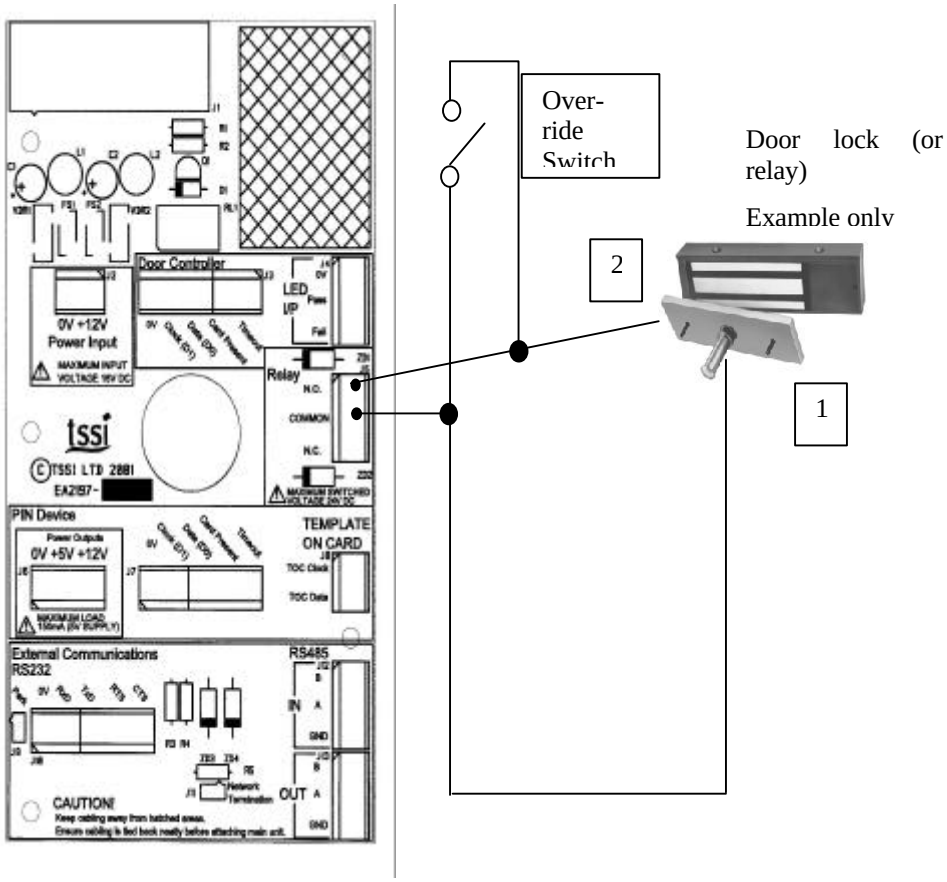


Figure 5 : Connecting a door lock driver (basic)

Delay and Strike times are pre-set to the following values:

DELAY – the time period after verification is complete before *Verid+* sends the DOOR OPEN signal - set at 0 Seconds, i.e. no delay.

STRIKE - the time period after verification for which the DOOR OPEN signal is energised i.e. the time for which the door is open - set at 4.5 Seconds.

Be aware that when *Verid+* is operated in this mode you will **not** have:

- Any control of Access rights. All verified users in the database will be able to gain entry.
- Any time rights, e.g. entry cannot be blocked between 18.00 and 07.30.

If either of these functions are required then a full Access Control System must be used.

Verid+ units used to control local doors can be networked in a similar way to *Verid+ units* used as part of a centralised Access Control System.

4.8 Error codes output by Verid+

Depending on the type of PIN device being used with *Verid+*, the error code output when a fingerprint fails to be matched against the stored template is as shown below. Note: the error code is also sent out when a card or pin number which is not in the database is used.

PIN device		No. leading zeros.	Start sentinel	Data (decimal)	End sentinel	LRC present?	No. trailing zeros.
Wiegand 2601		N/A	N/A	000000	N/A	N/A	N/A
Wiegand general		N/A	N/A	000000	N/A	N/A	N/A
Track 2		10	B (hex)	000000	F (hex)	Yes (= 8)	10
Watermark		10	10011111101 (bin)	000000	1 (bin)	No	10
Keypad		10	B (hex)	000000	F (hex)	Yes	10

Table 5 : Error codes output by *Verid+*

4.9 Terminal block connections and pin-outs.

All connections to and from *Verid+* are made using the terminal block on the rear plate. All connections are listed in the table below:

Block Number	Terminal Label	Section	Function	Block Numbe	Terminal Label	Section	Function
J2	OV	Power input	Power Supply Input: OV	J8	TOC Clock	Template-on-card	Template-on-card Clock
J2	+12V	Power Input	Power Supply Input: +12V	J8	TOC Data	Template-on-card	Template-on-card Data
J3	OV	Door Controller	OV (for door controller)	J9	Park	RS485	Storage for Network Termination Jumper for RS485
J3	Clock (D1)	Door Controller	Output to door controller Clock or Wiegand '1'	J10	OV	External RS232 Comms	OV for RS232
J3	Data (D0)	Door Controller	Output to door controller – Data or Wiegand '0'	J10	RxD	External RS232 Comms	Receive for RS232
J3	Card Present	Door Controller	Output to door controller – Card present	J10	TxD	External RS232 Comms	Transmit for RS232
J3	Timeout	Door Controller	Output to door controller - Timeout	J10	RTS	External RS232 Comms	Request to send – RS232
J4	Ov	LED I /P	OV (for LED Control)	J10	CTS	External RS232 Comms	Clear to send – RS232
J4	Pass	LED I /P	External LED Control PASS LED	J11	Network Termination	RS845	Network Termination Jumper for RS485
J4	Fail	LED I /P	External LED Control FAIL LED	J12	A	RS485 IN	RS485 – A Wire IN
J5	N.O.	Relay	Normally open contact	J12	B	RS485 IN	RS485 – B Wire IN
J5	Common	Relay	Common for relay	J12	GND	RS485 IN	Ground for RS485
J5	N.C	Relay	Normally closed contact	J13	A	RS485 OUT	RS485 – A Wire OUT
J6	OV	PIN Power Output	Output to external device : OV	J13	B	RS485 OUT	RS485 – B Wire OUT
J6	+5V	PIN Power Output	Output to external device: 5V	J13	GND	RS485 OUT	Ground for RS485
J6	+12V	PIN Power Output	Output to external device: 12V				
J7	OV	PIN Device	OV (For PIN Inputs)				
J7	Clock (D1)	PIN Device	Input from PIN-Clock or Wiegand '1'				
J7	Data (D0)	PIN Device	Input from PIN Data or Wiegand '0'				
J7	Card Present	PIN Device	Input from PIN – Card Present				
J7	Timeout	PIN Device	Input from PIN - Timeout				

5 Changing the way the unit is configured (*Verid* Manager)

5.1 General principles – SuperUsers, Supervisor and Configuration

In addition to the everyday users who use the unit to gain access there are three other important categories of user:

a) SuperUser - can enrol new users, or update a user's templates on a *Verid+* enrolment unit. Access to perform these (and other) functions is gained by holding the CANCEL button whilst entering their PIN and subsequently verifying the SuperUser's identity with their fingerprint.

b) Supervisor - can add, delete and transfer templates between *Verid+* units, as well as change some of the basic options available on the units. Access to the Supervisor mode is via a serial device connected to the integral RS232 port on all *Verid+* units and is password protected. (This mode is normally accessed by the on-site system manager)

c) Configuration - enables the *Verid+* units to be configured to suit the specific system requirements, for example the input and output data formats, database location, verification or enrolment, etc. Access to the Configuration mode is via a serial device connected to the integral RS232 port on all *Verid+* units and has separate password protection. (This mode is normally accessed by the system integrator/installer)

NOTE:

The Verid Manager kit provides all the listed Supervisor and Configuration commands. A full description of Verid Manager is given in TSSI document OM201.

5.2 SuperUser

A SuperUser can access a number of functions using the four control keys and the LCD screen. "SuperUser" Mode can be accessed, ***by SuperUsers only***, by depressing the "CANCEL" (X) key for the ***entire*** duration of the PIN entry. *Verid+* will then verify the identity of the user by requesting a fingerprint as normal. Once the identity has been verified, the SuperUser can perform the following actions.

Add a new user	Update an existing user	Delete a user

Using these options is explained in sections 6.4 and 6.5.

5.3 Supervisor – option commands

Once *Verid+* has been connected to a PC, using e.g. *Verid* Manager, the following commands are available to a "Supervisor". Within *Verid Manager* the supervisor mode is entered from the Mode drop down menu. This displays the Password screen. (The Default password is "SysManager" - Note the use of Capital letters S & M).

- **Supervisor Options.** NOTE: selections shown in **BOLD** text below represent the factory default configuration. Alternative configurations can be saved to or loaded from a PC as configuration (.cfg) files.

  > **Selection of Security Level** (PIN only, Any fingerprint, 1 (lowest), 2, **3 (default)**, 4 and 5 (highest).

  > **Enable Second Templates**

  > External LED Control

  > **Automatically enter SuperUser mode on Power Up** (N.B. only when database is empty)

  > **Display verification result on LCD**

Database Management

Manipulation of the database is a Supervisor function and can be performed via the RS232 port. Details of data transfer options are given in Section 6.2 of the *Verid Manager* manual (OM201).

- **Start Verification.** Puts the unit into Verification Mode (and should also be used to exit Supervisor or other modes).
- **Start Enrolment**. Puts the unit into Enrolment Mode (SuperUser Mode and exits Supervisor mode). Equivalent to entering the PIN with the *Verid+* Cancel button pressed, when in Verification mode.
- **Start Transparent.** Puts the unit into Transparent Mode (and exits Supervisor mode). Transparent mode is equivalent to connecting the PIN device direct to the door control unit.
- **Change Password.** Changes Current (Supervisor) Password
- **Update software.** Allows download of new *Verid+* unit software

5.4 Configuration – option commands

Configuration can be performed with *Verid Manager* via the RS232 port. Within *Verid Manager* the configuration mode is entered from the **Mode** drop down menu. This displays the Password screen. (The Default password is "Config" - ***Note the use of Capital letter C***).

A new screen will appear and the following selections are available via the drop down menus:

- **Connection**
- **Mode**
- **About**.

Select **Connect**, and the COM port where the D Type cable is connected. Confirmation that communication has been established is shown by the message "Connected" appearing in the bottom right hand corner of the window along with text in the Unit Software Version box.

Additional options become available from the menu bar headings:

- Connection	**- Disconnect**	Closes Serial Port
	- Check Connection	Checks the Connection to *Verid+*
- Mode	**- Supervisor**	Switches into Supervisor Mode
	- Configuration	Switches into Configuration Mode
	- Start Verification	Puts unit into Verification Mode and should also be used to exit Configuration)
	- Change password	Changes Current (Configuration) Password.
	- Update software.	Allows download of new *Verid+* unit software

- Options

- Configuration Options. Allowing Save, Load, Apply and Retrieve of various configuration settings as listed below:

> *Hardware options*:

- ➢ LCD screen fitted
- ➢ Menu keypad fitted
- ➢ Location of verification database

> *Enrolment options*:

- ➢ Enable as enrolment unit
- ➢ Source of new PIN
- ➢ Enrolment database location
- ➢ SuperUser database location

> *Input & output options*:

- ➢ Select PIN device
- ➢ Enable CardPresent
- ➢ Enable TimeOut

> *Network options*:

- ➢ Transmit configuration information
- ➢ Automatic configuration enable
- ➢ Transmit database records
- ➢ Receive database records
- ➢ Transmit enrolment commands
- ➢ Set network ID (if applicable)
- ➢ Enable power up checks
- ➢ Enable LED output

- Messages View / change the unit's LCD messages with Save, Load and Retrieve facilities, see section 5.5.

- Database

- Erase database Erases the entire database from the *Verid+* unit. Note to perform this task the Configuration password must be entered.

5.5 LCD text – changing the displayed messages

The text displayed on the LCD screen of each enrolment unit can be customised for a particular user either by using *Verid Manager* or via the RS232 commands in TSSI document OM205.

The display fitted to standard *Verid+* units is a Hitachi 5x7 dot matrix display, fitted with the Hitachi HD 44780 controller. Full details of the available character set can be found in the Hitachi datasheet.

PLEASE NOTE: If *Verid Manager* is being used, some characters (e.g. with accents or umlauts) displayed on the PC may not always correspond to what is displayed on the LCD screen of *Verid+*. The exact appearance will depend on how Windows has been configured on the PC.

TSSI have some configuration files to convert the standard messages into different languages – please contact TSSI for an up to date list of available languages.

Languages currently available include:

English, French, German and Portuguese.

6 Using the unit for the first time

6.1 Important concept – "Users" and "SuperUsers"

SuperUsers can enrol new users, or update a user's templates on a *Verid+* unit. Access to perform these functions is gained by holding the CANCEL button whilst entering their PIN and subsequently verifying the SuperUser's identity with their fingerprint.

Users have no ability to alter anything within *Verid+*. Users simply verify themselves against their PIN.

6.2 Important concept – "Security Levels"

Security levels can be assigned to users, SuperUsers as well as the *Verid+* unit itself. The security level assigned to the *Verid+* unit is termed a "global" level. A user (or SuperUser) assigned a security level of "global setting", will be checked to the security level assigned to the *Verid+* unit they are using. ***In all cases, the user's security level takes precedence over the Verid+ unit's security level.***

6.2.1 Global Security Levels for *Verid+* units

Each *Verid+* unit can be set to any of the following global security levels:

PIN only	No fingerprint is required – user only swipes card, or keys in PIN.
Any fingerprint	No fingerprint match is performed but the user is required to place a finger on *Verid+*.
Level 1	Lowest security.
Level 2, 3 & 4	Increasing security. (Level 3 is the default setting)
Level 5	Highest security.

Table 6 : Global security levels for *Verid+* units

6.2.2 Security Levels for individual users

Each *Verid+* user can be set to any of the following security levels:

Global setting	User is tested against the security level within *Verid+*.
PIN only	No fingerprint is required – user only swipes card or keys in PIN..
Any fingerprint	No fingerprint match is performed but the user is required to place a finger on *Verid+*.
Level 1	Lowest security.
Level 2, 3 & 4	Increasing security. **(Level 3 is the default setting).**
Level 5	Highest security.

Table 7 : Security levels for individual *Verid+* users

6.2.3 High **Security** Mode

As a further aid for users who have applications where the ultimate performance is required a new mode has been added. This is called “High Security mode”. This mode uses several special functions to enhance performance, amongst them is function that enhances the quality of poor quality templates.

It should be noted that whilst “High Security mode” enhances performance, it does so at the expense of usability. Positioning of the finger on the optics plate during enrolment becomes more critical – the finger must be placed with greater accuracy to achieve an acceptable enrolment score. Positioning of the finger on the optics plate during verification also becomes more critical – the finger must be placed with greater accuracy to get a pass.

The factory default setting for “High Security mode” is OFF. It can be switched ON by using Verid Manager VM5.01. Unlike the other Security levels the “High Security mode” can only be accessed using Verid Manager.

6.3 Tips when using biometric systems

Biometric systems measure a unique characteristic of an individual. In general these characteristics are not absolutely fixed and vary with time. For example temperature and humidity affect the size and shape of fingers, lighting, viewing angle and mood affect a person’s face etc. Consequently a biometric system has to make a judgement about how well a measurement (template) compares with a previously stored template.

The accuracy and reliability of the fingerprint verification process can be improved by ensuring the fingers are placed consistently, in the case of *Verid+* placed down onto the platen towards the top of the finger guide. Examples of good and bad finger placement are shown below.

Figure 6 : Good finger position – straight and in contact with the back of the finger guide

Figure 7 : Bad finger position – finger not pushed back fully.

Figure 8 : Bad finger position – finger rotated.

Do The finger should cover the glass area with the finger just touching the end of the fingerguide. The finger should be pressed reasonably firmly straight down.

Don’t **Do NOT slide the finger into the guide.**

Do NOT put the finger into the guide as shown in Figure 7 or Figure 8. Do not press excessively hard – it’s not necessary!

N.B. **If some users have persistent problems with successful verification then they should be re-trained and re-enrolled. In extreme cases where users have poor fingerprint definition it may be necessary to assign them a lower security setting.**

6.4 Enrolling the first SuperUser

Each new unit is supplied with no users enrolled and will automatically enter SuperUser mode on power-up. The LCD text will briefly display “Entering SuperUser mode” before showing “Add a new user”. A series of different options can now be selected by using the arrow keys:

Down arrow **Up arrow** **Enter** **Cancel**

Once in SuperUser mode, the first person to enrol **must** enrol as a SuperUser.

N.B. The unit will automatically exit SuperUser mode if, at any time, no key is pressed for 30 seconds.

1. Power up the unit. *Verid+* will automatically enter SuperUser mode. Dependant on the version of *Verid+* software used, some changes to the routine outlined below may apply. Press “ENTER”.
2. When “Add a new user” is displayed, press “ENTER”.
3. When “Enter NEW PIN…” is displayed, swipe card or key in PIN number. Press “ENTER”
4. Use the down arrow key to select “Super-User” and press “ENTER”. (***DO NOT*** select Normal user).
5. *Verid+* will then request a security level *for the new user*. When “Global setting” is displayed, press “Enter”. Use “Global setting” until familiar with concept of security levels.
6. Place finger in the finger guide (see Figure 6, page 22) until the “Busy” light shows.
7. Remove finger.
8. Repeat steps 6 and 7 twice more.

   (The message “”Enrolment score”” is briefly displayed before reverting to the message “Add new user”.) See section 6.4.1 below for details of enrolment scoring.
9. If second templates are enabled, the message “Define user’s second template” is displayed. Press “ENTER” to enrol second template, or “CANCEL” if not required.
10. Repeat steps 2 to 9 again if any other users are to be enrolled, otherwise use the down arrow key to select “Save all changes and exit”. ”Enrolment score” is also shown for 2nd templates.
11. Press “ENTER”. If the *Verid+* units are networked together, all new templates will be broadcast once the “ENTER” button is pressed.

Notes for Keypad users: There are two ways within *Verid+* of entering a new PIN from a keypad. The first (factory default) method is for the user to choose and enter their PIN. The newly typed PIN will be checked against all previously enrolled PINs and inform the user if the PIN has already been assigned. Alternatively, *Verid+* can be configured to generate a random PIN by selecting one from those unused. Changing *Verid+* to generate random PINs can be done using *Verid Manager* (OM201) or via the RS232 specification (OM205).

N.B. ***Data on newly enrolled people is only stored permanently if the SuperUser mode is exited as described above.***

6.4.1 Enrolment scoring

After the enrolment sequence for the first and/or the second finger is completed Verid + displays the Enrolment Score. This Enrolment Score is a measure of the quality of the template formed, and has been included to encourage better quality enrolment. The Enrolment Score is on a scale of 1 to 10 but in practice only the higher numbers are displayed (10, 9, 8, 7, or 6) . An Enrolment Score of 10 is excellent, 9 is good, 8 is OK, 7 or below try again.

It is perfectly possible to attain a score of 10/10 for most enrolments although there will always be problem users who are unable to get a score as high as this. The scoring does help to identify these users so that appropriate measures can be taken to improve usability for them. These measures include setting a lower individual security level, and/or enroling the same finger as BOTH first and second templates.

You should note that as the security level is increased it becomes progressively harder for some users to use the system. At the higher security levels the discrimination of the system means that greater accuracy in finger placement is needed to achieve a PASS.

6.5 Enrolling all other people

Only a SuperUser can enrol additional users or SuperUsers. A SuperUser can enrol other users and SuperUsers by following the steps below:

1. Enter PIN or swipe card whilst depressing the “Cancel” button.
2. Place finger on the finger guide, if fingerprint is verified, the display will show “Entering Super-user mode”. Press “ENTER”
3. Once “Add a new user” is displayed, press the “Enter” key
4. Swipe new user’s card or enter PIN.
5. Use the arrow keys to select “Normal user” or “Super-user” and again press the “ENTER” key.
6. Now set the security level to be assigned ***to that user***. Until familiar with the concepts, select “Global setting” and press “ENTER”.
7. Place finger at the top of the finger guide on the plate until the “Busy” light shows.
8. Remove finger.
9. Repeat steps 5 and 6 twice more.(The message ”Enrolment score”” is briefly displayed before reverting to the message “Add new user”.) See section 6.4.1 for details of enrolment scoring.
10. If second templates are enabled, the message “Define user’s second template” is displayed. Press “ENTER” to enrol second template, or “CANCEL” if not required.
11. When “Add a new user” is displayed, press “ENTER” to enrol further users or use the arrow keys to select “Save all changes and Exit”, then press “ENTER”.

Notes for Keypad users: There are two ways within *Verid+PIN* of entering a new PIN from a keypad. The first (factory default) method is for the user to choose and enter a new PIN. The newly typed PIN will be checked against all previously enrolled PINs and inform the user if the PIN has already been assigned. Alternatively, *Verid+PIN* can be configured to generate a random PIN by selecting one from those unused. Changing *Verid+PIN* to generate random PINs is explained in the RS232 specification document OM205 or document OM201 using *Verid Manager*.

N.B. ***Newly enrolled users will only be added to the database after exiting SuperUser Mode as described above.***

6.5.1 Using the “Update an existing user” option.

A ***SuperUser*** can change the properties associated with any enrolled user or SuperUser. These properties are:

- “User type” - Making the user a SuperUser or vice versa.
- “Security Level” - Assigning a different security level to this user (or SuperUser).
- “Define user’s template” - Updating the user’s first or secondary template.

Note: Only one of the above attributes can be changed at a time, see step 6 below if more than 1 attribute needs to be changed.

In all cases, the procedure is the same:

1. A SuperUser should enter a PIN or swipe card whilst depressing the “Cancel” button.
2. Use the arrow keys to select “Update an existing user” and press “Enter”
3. When “Enter PIN” is displayed, swipe the card or enter PIN ***of the user that you wish to update***.
4. Use the arrow keys to select the property that you want to change – i.e. “Select user type”, “Select security level”, “Define user’s first template” or “Define user’s second template”, then press “Enter”.
5. Once e.g. “Select security level” has been selected, use the arrow keys to choose the new setting e.g. for security level this would be “global setting”, “Pin input only”, “Any fingerprint” or “Level 1” to “Level 5”. Choose the appropriate option and press “Enter”.
6. The screen will then return you to the “Add” / “Update” / “Delete” / “Exit” menu level. Repeat from step 2 again if any other of the users attributes need to be changed. Alternatively, select “Exit” then press “Enter”.

N.B. ***If a user is enrolled as PIN only then they cannot be converted to another security level later. To change from PIN only entry to PIN plus fingerprint, first delete the user from the unit and re-enrol with the same PIN. If an update is attempted an error message such as “bad finger for enrolling” will be displayed.***

7 Adding and Deleting users – Template Database Management

7.1 Overview - Template transfer

Template transfer between units can be done via RS232 using *Verid Manager* (a software package available from TSSI which runs on a PC), or using *Verid+*'s RS485 networking capabilities (see section 8).

All new enrolled templates are stored with their associated PIN within the *Verid+* enrolment unit. Templates can be transferred to other units via the RS232 interface. The RS232 connection is via a 3.5mm "stereo" jack connector on the underside of the unit.

Verid Manager, from TSSI, offers a variety of template management options. These include uploading and downloading the complete database or individual records. *Verid Manager* also enables database information to be saved to a PC for backup or transfer to other units. More details are available in the document "*Verid Manager* User Guide", see section 5 and TSSI document OM201.

7.2 Adding and deleting templates via the RS232 port

A 3.5mm jack socket on the underside of all *Verid+* units offers standard RS232 communication with external devices.

RS232 commands are available for manipulating the database within the *Verid+* unit via a standard RS232 connection. The commands enable individual records to be copied from the *Verid+* unit onto a PC, or from a PC to a *Verid+* unit. This enables template transfer from enrolment units to verification units. Commands are also available for transfer of complete databases to and from *Verid+* units.

NOTE: Templates can be stored in both the *Verid+* unit database and a PC database.

The following commands are available in the Supervisor section of Verid Manager.

Send database	Sends a database to the *Verid+* unit. Once selected the full set of selected template (.vdb) files will be copied from the PC to the *Verid+* unit.
Get database	Gets a database from the *Verid+* unit and stores on the PC.
Send user	Adds a single user to the *Verid+* unit selected by PIN number.
Get user	Gets a single user from the *Verid+* unit. If a PIN number is selected then the current file in the PC database will be updated with the latest template from the *Verid+* unit.
Examine users:	Gets information about the unit's database, e.g.
• **New User**	Enables the *Verid+* unit to be updated with a template from the PC database.
• **Retrieve**	Examines and recalls all the users in the *Verid+* unit database. **Retrieve** must precede the **Get**, **Update** or **Delete** options.
• **Get User**	Enables template to be selected from the retrieved list and copied to the PC database.
• **Update User**	Enables an existing template on the *Verid+* unit to be updated with a template stored on the PC database.
• **Delete User**	Deletes a user's template from the *Verid+* database.
• **Erase Database**	Erases the entire database from the *Verid+* unit.

7.3 Emptying the database – Verid Manager

The ability to completely empty the internal database is important for installation and testing of *Verid+* units. When the internal database is empty the *Verid+* units revert to the SuperUser mode. This means the first user to enrol becomes a SuperUser and can enrol additional new users and SuperUsers.

The internal database of a *Verid+* unit can be completely erased through either the Supervisor or Configuration Modes:

a) *Supervisor Mode* - to enable the system manager to empty a *Verid+* unit after installation, commissioning and acceptance from the system integrator. Erase Database is available under the Database pull down menu of *Verid Manager*

b) *Configuration Mode* - during installation and testing a system integrator will wish to enrol on and use the *Verid+* units. After installation and commissioning the system integrator can empty the database ready for use by the system manager. Erase Database is available under the Database pull down menu of *Verid Manager*

If you are on a network the database will be replaced by other units on the network unless you disable BOTH receive and transmit template boxes before erasing the database.

7.4 Managing the database – Verid Manager

It is strongly recommended that normal database management practices be followed to ensure recovery of data in the event of a disaster. Good practise would include the regular downloading of the database from the enrolment units to a PC, with a backup of the database stored on portable media in a fireproof safe, ideally on a remote site. Should new units be added to the system, the database can be immediately uploaded.

8 Guidelines - Networking *Verid*+ units.

Setting up and operating a network of *Verid*+ units has been designed to be simple. No PC is needed to set-up or operate the network and once running, some of the operations that will take place automatically include:

- Automatic database synchronisation across all the networked units.
- Adding, updating and deleting a user (or SuperUser) via the control keys will initiate an immediate broadcast of the new template details to all units on the network.
- A new unit added to the network will automatically adopt the configuration of the other units on the network, e.g. PIN device, security level, passwords, messages. This will only occur if "Autoconfigure" is enabled.

8.1 Installing (wiring) a Verid+ network

The diagram below shows the wiring arrangement for setting up a network.

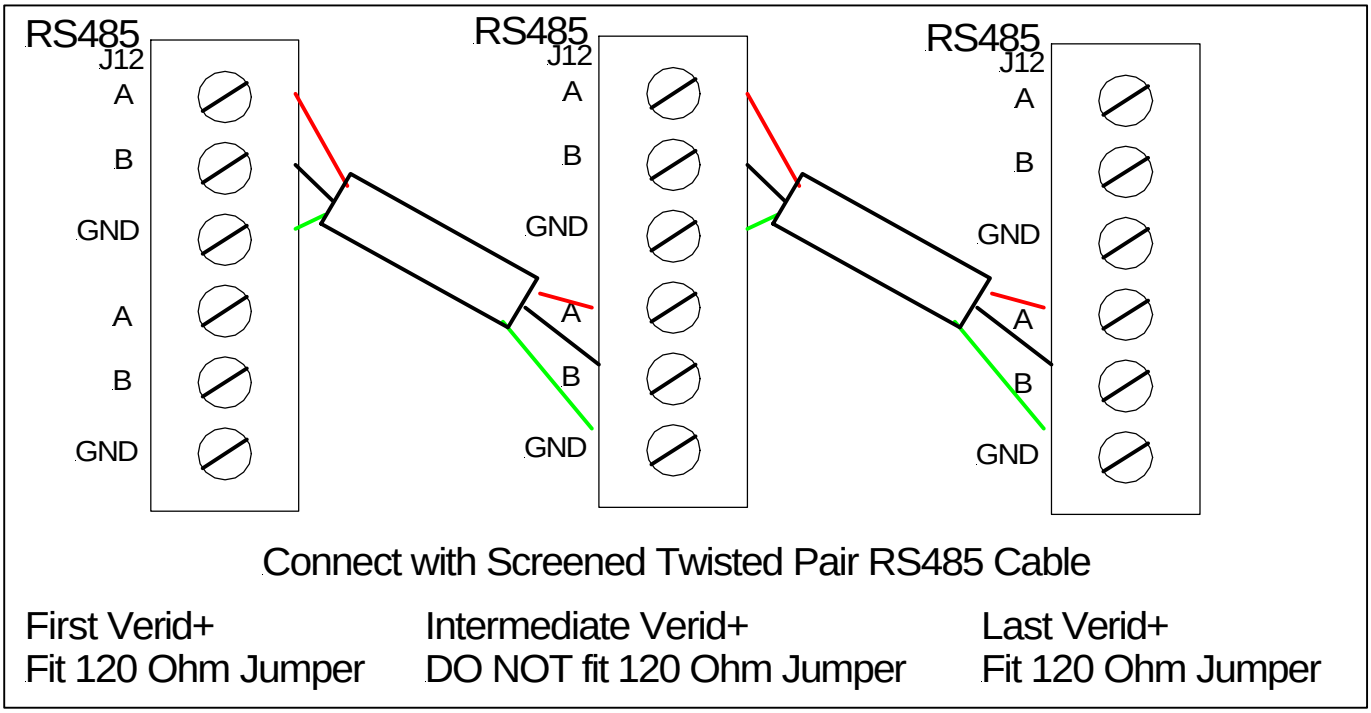
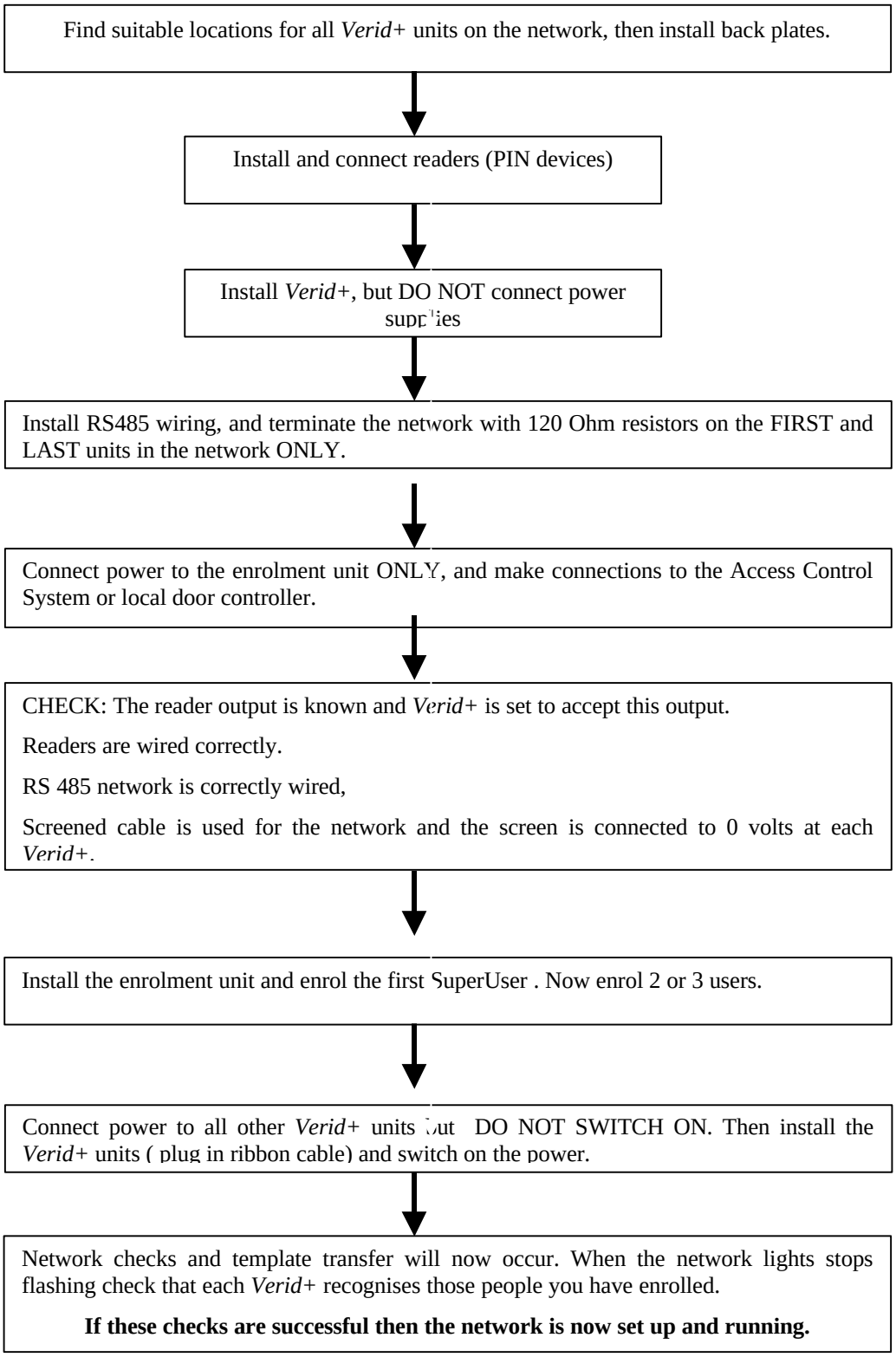


Figure 9 : *Verid*+ network wiring

Please note:

1. No network "spurs" are allowed.
2. Ensure the 120 Ohm termination resistors are selected by the jumper at each end of the line.
3. Use cable which is correctly specified, see section 8.7

8.2 Setting up a *Verid+* network without reading the manual.


Find suitable locations for all *Verid+* units on the network, then install back plates.
Install and connect readers (PIN devices)
Install *Verid+*, but DO NOT connect power supplies
Install RS485 wiring, and terminate the network with 120 Ohm resistors on the FIRST and LAST units in the network ONLY.
Connect power to the enrolment unit ONLY, and make connections to the Access Control System or local door controller.
CHECK: The reader output is known and *Verid+* is set to accept this output.
Readers are wired correctly.
RS 485 network is correctly wired,
Screened cable is used for the network and the screen is connected to 0 volts at each *Verid+*.
Install the enrolment unit and enrol the first SuperUser . Now enrol 2 or 3 users.
Connect power to all other *Verid+* units but DO NOT SWITCH ON. Then install the *Verid+* units (plug in ribbon cable) and switch on the power.
Network checks and template transfer will now occur. When the network lights stops flashing check that each *Verid+* recognises those people you have enrolled.
If these checks are successful then the network is now set up and running.

8.2.1 Verid+ Network – getting started / overview

NOTE: All units on a network MUST be of the same type: i.e. all with keypad all with track 2 magswipe or all with proximity readers.

Once a network in has been installed using new *Verid+* units, it is first necessary to configure ONE of the units to the desired configuration (e.g. PIN device, language of messages etc.) using *Verid Manager*. Once the configuration changes have been made, it is essential to clear the "Automatic configuration enable" checkbox (see Figure 10).

Having made the changes to the configuration and "Automatic configuration enable" checkbox, power down any one of the units on the network. On power-up, the other units on the network will be automatically configured to adopt the settings of the unit which has its "Automatic configuration enable" check-box cleared.

Once the network is running, the *Verid+* units will communicate with each other on a peer-to-peer basis with all messages being sent and received by all units.

N.B. A *Verid+* unit with a unique address set will still respond to broadcast commands.

Once the network has been established, the following will happen automatically:

- If a new user (or SuperUser) is added, or has their template updated, the new template(s) will be immediately and automatically broadcast to all units on the network on exiting SuperUser mode.
- If a user is deleted using the four arrow keys, the deletion is broadcast immediately to all units on the network.
- The first time a new unit (with factory default configuration) is fitted onto an existing network, it will automatically adopt the configuration, messages and templates of all the other units on the network. (This feature can be disabled, see section 8.8).
- If any of the *Verid+* units on the network is temporarily disconnected, it will, on re-connection, be updated with any templates added or updated during the period it was off-line. Synchronisation of the databases happens automatically and is verified on a frequent basis.
- Any changes to the security level or status of a user (or SuperUser) will be broadcast to all networked units.
- A PC running *Verid Manager* can be used to resolve any problems – see section 8.8.

8.3 Verid+ Network – power up LED sequencing

After a *Verid+* unit is powered up, the LCD will display the version number and some other messages. Once these are complete, the "Network tests" are performed (if previously selected as a network configuration option) during which the red and green LED's flash continuously. The network tests will check the ID status (to resolve any network address conflicts), configuration details (e.g. PIN device, message text etc.) and the database consistency of the networked units.

In general, the

- First Yellow LED indicates ***ID*** status
- Second Yellow LED indicates ***Configuration*** status. (See below for more details)
- Green LED indicates ***Database*** status. (See below for more details)
- Red LED indicates Network checking is taking place (see below for details)

After power-up, the LED's and LCD display will perform as follows:

1) Initially the "Self test passed " message will show on the LCD and the LEDs will flash in sequence from left to right.
2) The First Yellow LED flashes while IDs are reported. If a new ID has to be assigned to the unit, the LCD will blank for a short time whilst this is being done. The LCD display will then show the new ID and total number of units on the network (e.g. ID = 02/05).

3) The Second Yellow LED flashes while configurations are reported.

   If messages need to be transferred, the LED flashes slowly and goes off at end of a successful transfer. If a new configuration is received, the display will again blank.

4) The Green LED flashes while database states are reported. If a transfer is performed, the LED flashes slowly and goes out at the end of a successful transfer.

5) The RED LED flashes while any of the steps described in stages 2 to 4 are taking place.

If an error is detected, any of the three processes may restart. As they can run concurrently the LED display can be rather complex. Do not be alarmed: there is no reason to analyse the LED sequence in normal circumstances.

After the last transaction, the Red LED continues to flash for 10 sec.

Once the initial start-up LED activity is finished, ***the LEDs remain lit and are not cleared until the first PIN is input***. This allows the installer time to note the unit status and any errors.

If any of the LEDs remain lit after power-up, they have the following meanings:-

First Yellow "***ID***" LED ON:	No other units found, configuration and database checks not done.
& if Second yellow "***Configure***" LED ON:	Unit not already configured.
& if Green "***Database***" LED ON:	Database empty.

First Yellow "***ID***" LED OFF:	Other units found.
& if Second yellow"***Configure***" LED ON:	All units unconfigured or auto-config failure.
& if Green "***Database***" LED ON:	All databases empty or transfer failure.

If a unit has an ID = 0 it will always be re- assigned the lowest available ID.

If a unit has an ID > 0 then it will not be changed unless there is a clash with another unit, when one unit will give way and take the lowest available ID.

PLEASE NOTE: for the auto configuration to work properly, the flags 'LCD fitted', 'Menu keypad fitted' and 'Enable as enrolment station' must be set appropriately on ALL units. To make a unit auto configure, the 'Automatic configuration enable' flag must be set, the unit connected to one or more configured units, and ANY unit on the network must go through a power up sequence. All these flags can be set using *Verid Manager*. This type of auto-configure means that it is possible to introduce an unconfigured unit into a set of configured units, or to build a system of unconfigured units and add a configured unit last.) As standard, *Verid+ units* are shipped from TSSI in a state which allows this quick and easy auto-configuration.

8.4 Verid+ Network – auto-configure

When auto-configuring takes place, the following elements are transferred across the network to any ***unconfigured*** *Verid+* units:-

All units:
⇩
Input PIN device, format and flags.
Output PIN device, format and flags.
Global Security Level.
Messages - ***except*** messages 1 & 2 (“version number”) and 3 & 4 (“*Verid+* – a TSSI development”).
Supervisor password.
Configuration password.

In addition to the above configuration details, certain other details are sent depending on the exact configuration of each *Verid+* unit – as shown below.

All Units		**Keypad units only:**	
⇩		⇩	
New PIN source		Key PIN length	
Auto Enrolment flag		Keypad map	

If all configured units are consistent on a particular element, an unconfigured unit will adopt that setting, otherwise it will retain the setting already in use. If an element is not relevant to a unit, it will not report it - e.g. a unit that is configured for swipe input will not report the state of its keypad map.

8.5 Installing a simple Verid+ network

1. Ensure that any one enrolment unit is configured as required and working with the PIN entry device.
2. Use *Verid Manager* to clear the flag ***”Automatic configuration enable”. See section 8.8***
3. Enrol users and SuperUsers.
4. Connect the other *Verid+* units, following the wiring instructions given in Figure 10. Ensure termination resistors are selected at each end of the network. These units can be left in the default state and will then auto-configure.
5. Connect PIN entry devices to each new unit and reconnect power.

Once powered up again, the original unit, onto which people were enrolled, will transmit all templates to all other units on the network, and will also automatically configure each unit to set PIN device, security level and LCD messages ***to be the same as itself***. There will be some LED activity whilst this process is happening.

The network of *Verid+ units* will now continue to communicate to each other. If any unit is taken off-line, it will inform all the other units once it comes on-line again. It will be updated with any template additions / updates / deletions at this time.

8.6 Verid+ network – Adding additional units

Adding units to an installed system is a simple matter of wiring in the units following the guidelines shown in Figure 10. Once connected, the new unit will only assume the configuration parameters that are ***unanimous*** across all other units on the network. This includes PIN device, messages, etc. as explained in section 8.2.1. Those configuration parameters that are not unanimous are left in their factory default states.

If the address of the new unit conflicts with that of an existing unit, the networked *Verid+* units will resolve the conflict – however it may alter the address of an existing unit to do this!

8.7 Technical guidelines for installing an RS485 network

Recommendations:

Wire characteristics:	Twisted pair with overall screen.
Termination resistance:	120 Ohms (2 resistors required per site, one at each end of the network). Select using jumper
Maximum total number of *Verid+* units on network:	128
Architecture	Linear bus – NO SPURS.
Total cable length	(Cable dependent) but tested to over 500m.

Table 8 : Wiring details for *Verid+* networks

8.8 Using Verid Manager with networked units

Verid Manager enables the user to determine the way a *Verid+* unit interacts with the network. The "Network" screen from Configuration Mode / Configuration Options, is shown below:

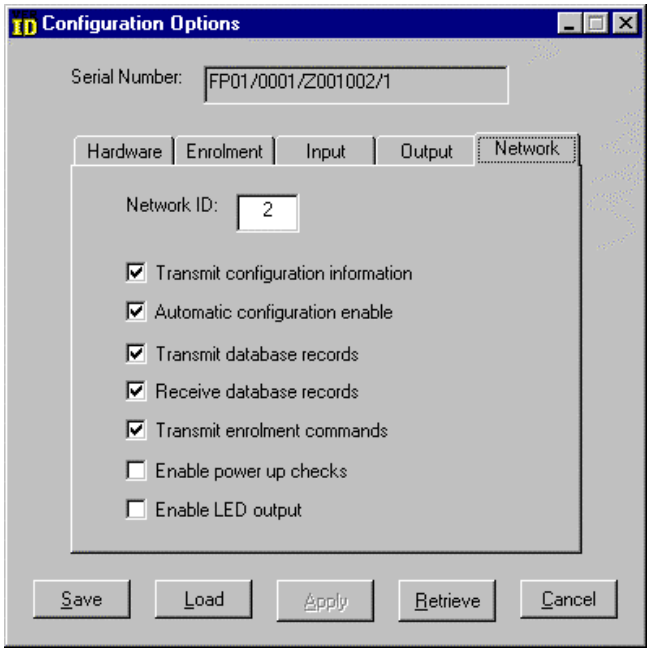


Figure 10 : *Verid Manager*– factory default network settings

Use this screen to change or enquire about the unit's address. Additionally, the five check boxes dictate how each *Verid+* unit will behave when connected to a network. The default on delivery is to have all check boxes ticked. Once a *Verid+* unit has been auto-configured by e.g. another *Verid+* on a network, the "Automatic configuration enable" checkbox will be cleared. In normal network operation, all except "Automatic configuration enable" should be checked. If there is a specialised requirement, each checkbox is explained below:

1. ***Transmit configuration information***: If checked, periodically the unit will inform all other networked *Verid+* units of it's configuration. Therefore it will affect the configuration of a new unit arriving on the network.
2. ***Automatic configuration enable***: If this box is checked, and the unit is placed onto the network, it will adopt the configuration of those units on the network which "***Transmit configuration information". N.B. one unit on the network must have this box cleared so that all other will adopt its configuration details.***
3. ***Transmit database records***: If checked, the unit will periodically inform other networked units of the contents of it's database. If other networked units are deemed to have an older or smaller database, and have "receive database records" checked, they will be updated.
4. ***Receive database records***: If checked, the unit will be updated with database information from other units on the network if they are deemed to have more recent database information.
5. ***Transmit enrolment commands***: If checked, each addition / update / deletion / change to security level or status of a user (or SuperUser) will initiate a broadcast of the new information to all other units on the network.
6. ***Enable power up checks***: If checked, then on power up the *Verid+* unit will communicate with the others on the network and adopt the default configuration details of the main units on the network.
7. ***Enable LED output***: If checked, then on power up the *Verid+* unit will signal the status of the network communications on the front panel LEDs whilst the unit is performing its network power up check routine.

9 Storing templates on magnetic cards

Verid+'s small template size (52 bytes) means that the template can be stored on a magnetic stripe card. Storing templates in this way, removes the need for ensuring database consistency across all installed *Verid+* units and removes the need for networking or PC template transfer.

At present this feature is available on magnetic stripe cards which conform to ISO 7811 standard. TSSI will promote the extension of this to other proprietary card technologies, and will support system integrators or card suppliers in making template storage possible on any card, token or data carrier.

9.1 Using templates on a magnetic card:

If templates are to be stored on a magnetic card, the card with the template MUST contain PIN data on track 2 and the template data on track 3, as shown in Figure 11 below:

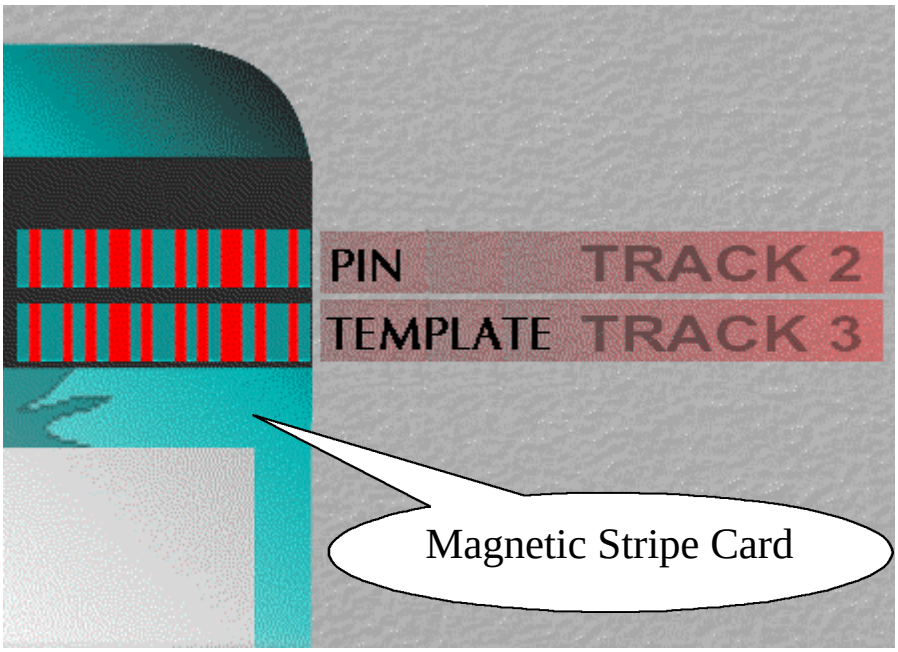


Figure 11 : Template and PIN on magnetic card

When the card is swiped, both tracks are read simultaneously and the data sent to *Verid+*, where the finger is verified against the track 3 template. If the match is successful, the PIN data (track 2) is output as normal. The card should be read with a track 2+3 reader with the output conforming to either OMRON or MAGTEK timings and the data on both tracks should conform to ISO 7811. The strobe and data lines for the PIN and template information should be connected to *Verid+* as follows: Track 2 PIN: connect to clock and data on J7. Track 3 template: connect to TOC clock and TOC data on J8. Use Verid Manager to select template source as Template on Card.

9.2 Generating and verifying track 3 templates using Verid+

A *Verid+* unit can be used to generate a template for encoding onto track 3. The RS232 command to generate the template is explained in document OM205. To verify the fingerprint against the template stored on track 3, *Verid+* must first be configured into the correct mode to receive the template from track 3. This is established using *Verid Manager* or via the RS232 command set, (see TSSI documents OM201 or OM205 respectively).

9.3 Encoding templates onto track 3

Once the RS232 command to create template has been issued *Verid+* will enrol a user as normal then reply (via the RS232) with the template. The template consists of 52 bytes of information. Converting this to the track 3 data is shown below using an example response to illustrate:

Example response from *Verid+* (hex data):

Header		Length		Identifier		Data		CRC
76 9A 4D C6		00 37		53		87 24 56 72 56 33 01 20 …etc		12 A4

Resulting track 3 card:

Leading zeros		Start Sentinel				Track 3 Data		End Sentinel
As ISO 7811		"B" (hex)				8 7 2 4 5 6 7 2 5 6 3 3 0 1 2 0 …etc		"F" (hex)

Each byte within the 52 byte template contains a BCD (binary coded decimal) representation of two decimal characters. The upper and lower four bits of each byte denote BCD characters. The first bit immediately following the ***identifier*** is the most significant bit of the first decimal character which itself should be encoded immediately after the start sentinel characters of the track 3 data. The template, once encoded onto track 3, is fully ISO 7811 compliant, with 104 decimal characters, plus start and end sentinels and LRC character.

10 Fault finding / Troubleshooting / Safety

10.1 Troubleshooting & frequently asked questions

WARNING - Do not perform any faultfinding / troubleshooting on this unit until you have read and understood the operating and safety instructions given in this manual.

Safety Instructions:

1. Electricity is dangerous. All maintenance should be carried out by competent and fully trained staff.
2. Access control systems must continue to allow rapid exit in the case of fire. In normal use, *Verid+* should control entry to the building but should not control exit. Always obey local fire regulations.

Fault Finding / Troubleshooting Chart:

Indication / problem	Possible Cause	Action
How do I enter SuperUser mode?		Only SuperUsers can enter SuperUser mode. Entering SuperUser mode is achieved by pressing the CANCEL key (on an enrolment unit only) during the entire duration of the PIN entry and verifying the fingerprint.
What are the default passwords?		Supervisor Mode = "***S***ys***M***anager" Configuration Mode = "***C***onfig" N.B. They are ***C***ase ***S***ensitive
All LEDs come on when I connect a external PIN device	PIN device is drawing too much current from the 5V supply.	Check wiring of the PIN device and then the current consumption against the current available from *Verid+*.
Card swiped – finger guide not illuminated	The card reader may not be operating correctly. Alternatively, there may be a difficulty decoding card data – e.g. due to card error, format error or swipe action.	Ensure the card reader is working correctly. Try re-swiping the card to ensure the card action is not causing the problem. Check wiring and data waveforms between card reader and *Verid+*. Check the configuration of *Verid+* is suitable for the card device being used.
Card swiped & finger recognised. Green "Unlock" LED lights green but door does not open.	PIN device and finger are being recognised. Problem is on "output" side of functionality of *Verid+* – or "input" to the access control system.	Likely causes of the door not opening are: Card number needs to be entered onto the access control system database. Check *Verid+* output is of the correct format for door controller.
As soon as card is swiped, the red "Lock" LED flashes, the finger platen does not become illuminated and LCD shows "invalid"	Card data cannot be decoded by *Verid+* or card is not on the *Verid+* database.	Try re-swiping the card again to ensure correct action. Check wiring and data waveforms between card reader and *Verid+*. Check configuration of *Verid+* is suitable for the PIN device being used. Ask a SuperUser to ensure that the card is held on *Verid+*'s database.
"Increase pressure" message shown on LCD.	Insufficient finger pressure. Insufficient area of fingerprint seen by *Verid+*.	Press harder and ensure correct finger placement. Alternatively, enrolling a different (broader)

		finger may be beneficial.
Cannot enter SuperUser mode even though CANCEL key is pressed.	Security level has been set to "PIN only" (Supervisor mode).	Enter Supervisor mode and change the security level to "Any fingerprint" or any of levels 1 to 5.
Units are connected onto a network but do not auto-configure	All networked units have the "Automatic configuration enable" flag set.	Use *Verid Manager* to clear the "Automatic configuration enable" flag on the unit which you want all others to learn their configuration from.

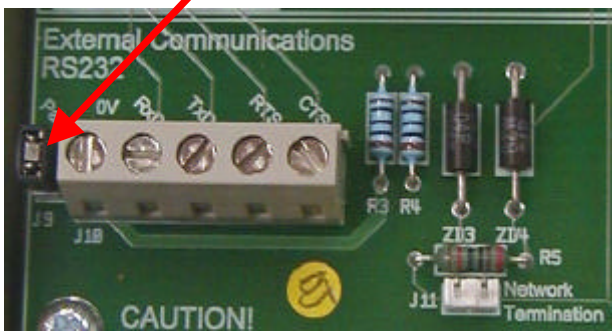


Figure 12 : Location of network jumper (park)

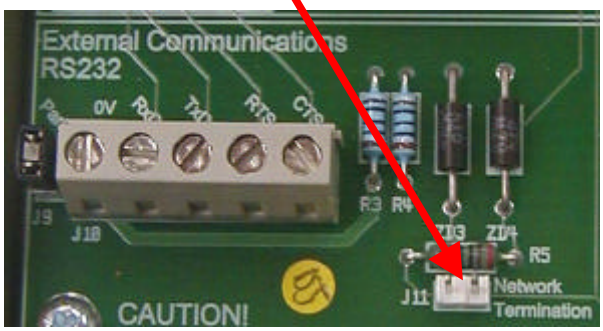


Figure 13: Location of networking jumper

10.2 Maintenance / spares / replacement parts

Verid+ is essentially maintenance free but will benefit from periodic cleaning of the optics and housing. Clean the finger platen with a soft lint free cloth. The housing may be cleaned with a soft cloth and non-abrasive liquid detergent.

There are no customer replaceable parts within *Verid+* Please contact TSSI for your nearest authorised repair centre.

10.3 Compatibility with earlier versions of Verid.

Verid+ units are compatible with Verid units running firmware version V4.06. No such compatibility is guaranteed with earlier firmware versions. The following information applies to Verid only and is included only for circumstances where it is intended to add *Verid+* units to a network of Verid units:

The way in which the fingerprint template is formed was changed at *Verid* Version 4.0, and it is important to understand the implications of this change.

Verid units using software version V3.31 and all earlier software versions (V3.02 etc) use 'type 1' templates. These *Verid units* create type 1 templates and only recognise type 1 templates. Care is needed in adding new *Verid units* to any sites where V3.31 or earlier is already installed.

Verid units after V4.0, including the current version V4.01, create type 2 templates but can recognise both type 1 and type 2 templates. This means that version V4.01 *Verid units* can be used as verification units on sites which have V3.31 (or earlier) enrolment units. Version V4.01 or later *Verid units* **must not be used** as enrolment units on sites which have V3.31 (or earlier) *Verid units.* This is because V3.31 will not recognise the type 2 template created by V4.01.

If a new enrolment unit is needed on a site, which uses earlier Verid units, then an alternative version called V3.41 is available. *Verid* units running V3.41 create type 1 templates and recognise both type 1 and type 2 templates.

Any problems associated with incompatibility of templates are indicated by simultaneous flashing of the hold, increase and decrease lights, the display will show a “Template not defined” message.

If there is any doubt about how to add *Verid* or *Verid+* units to an installation please contact TSSI for advice.

11 A technical overview

11.1 Fingerprint matching algorithm

Verid+'s fingerprint matching algorithm utilises a unique autocorrelation technology. The image captured from the fingerprint is electronically cleaned and enhanced and temporarily stored in *Verid+*'s memory. An exact electronic duplicate is created and overlaid on the original. By displacing the copy over the original in a prescribed manner a series of Moiré fringes are created. Analysis of these fringes characterises the fingerprint and a numeric template is created and stored against the input PIN number. Once the template is created the original images are discarded.

This autocorrelation approach relies on macro features of the fingerprint, rather than looking for minute detail, and is therefore more tolerant of finger damage. The resulting template is small, enabling storage on a single track of a magnetic stripe card.

As the template relates only to macro effects of the fingerprint, there is no way that the data stored by *Verid+* can re-create an image of a fingerprint that could then be used for forensic purposes.

11.2 Maximum number of users

Each *Verid+* unit can store data on up to 5000 people. Each of the 5000 people can have either one or two templates enrolled. The 5000 people can be any mix of users or SuperUsers.

11.3 Special Features

Information Mode (Switchable Option)

At software version VP 5.01 a new mode has been added – "Information Mode" This is a mode which is useable only on Verid +PIN, or Verid + with an appropriate external keypad. Information Mode allocates the * key to indicate that a person is entering an area and the # key to indicate that a person is leaving an area.

Verid + reports each transaction (Pass or Fail) via a data string transmitted from the RS232 port. With Information Mode OFF the PIN is one of the pieces of data transmitted. With Information Mode ON the 0ne extra character denoting IN is added to the PIN, and a different character is added to denote OUT. This mode is only used in specialised applications and has no use unless used in conjunction with other appropriate TSSI software/hardware. The default setting for Information Mode is OFF. It can be switched on using Verid Manager VM5.01.

11.4 TTL signal timing diagrams

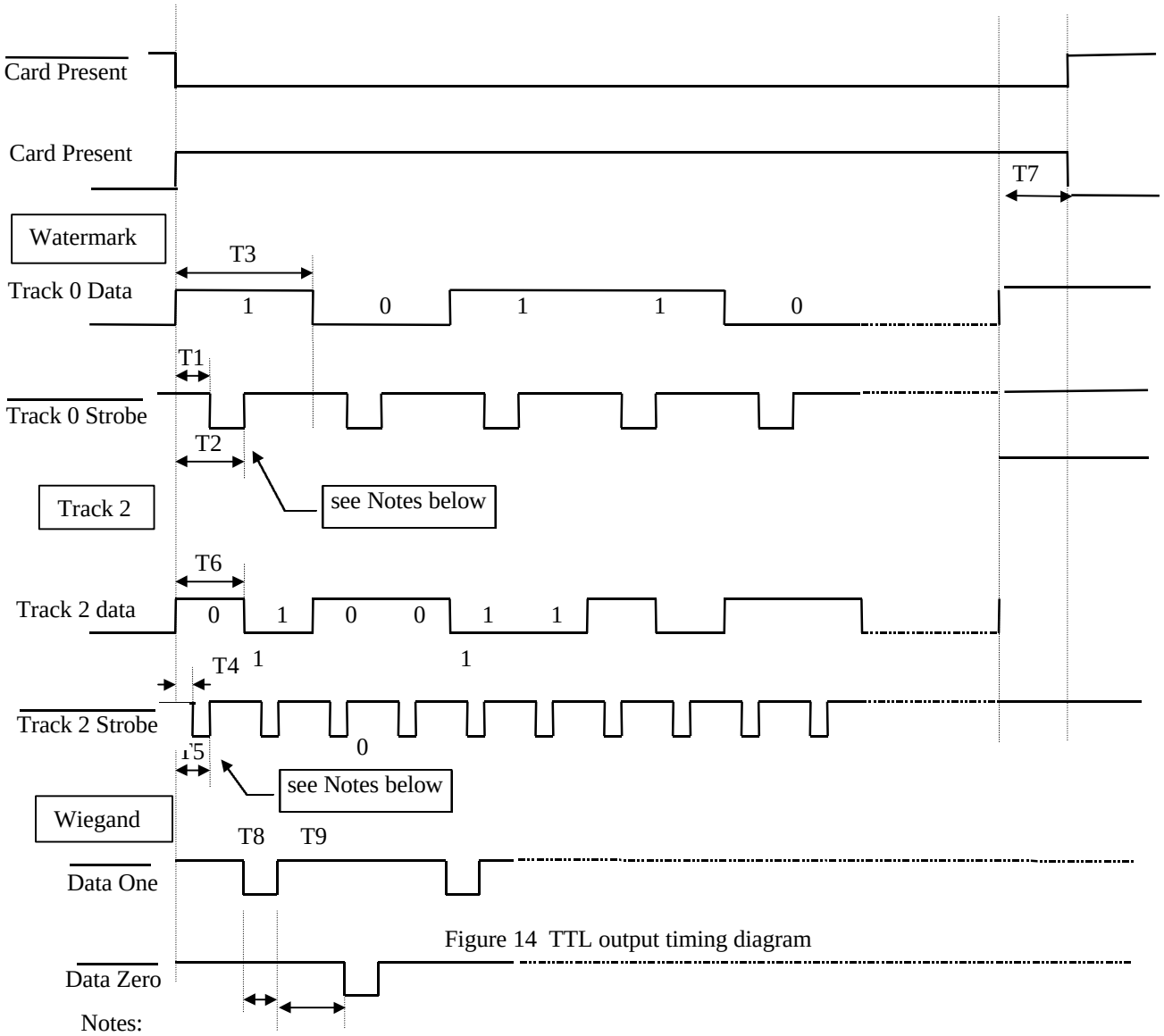


Figure 14 TTL output timing diagram

Notes:

1. The Data (out) line should be sampled on the falling edge of the strobe signal.
2. The position of the strobe pulse varies dependant on the reader type used. For OMRON the pulse is in the last 1/3rd of the bit period whilst for Watermark and MAGTEK readers it is within the first 1/4 or 1/2 of the bit period.
3. Only part of the signal package is outlined above for each signal line and the actual sequence of '0' and '1' bits shown is for illustrative purposes only.

SIGNAL LINES	TRACK 2		TRACK 0 WATERMARK	WIEGAND 2601
	OMRON	MAGTEK		
Card Present	___ (= CLS)		✕	✕
Card Present	✕	✕		✕
Track 0 Data	✕	✕		✕
Track 0 Strobe	✕	✕		✕
Track 0 Clock	✕	✕		✕
Track 2 Data	___ (= RDP)		✕	✕
Track 2 Strobe	___ (= RCP)		✕	✕
Data One	✕	✕	✕	
Data Zero	✕	✕	✕	

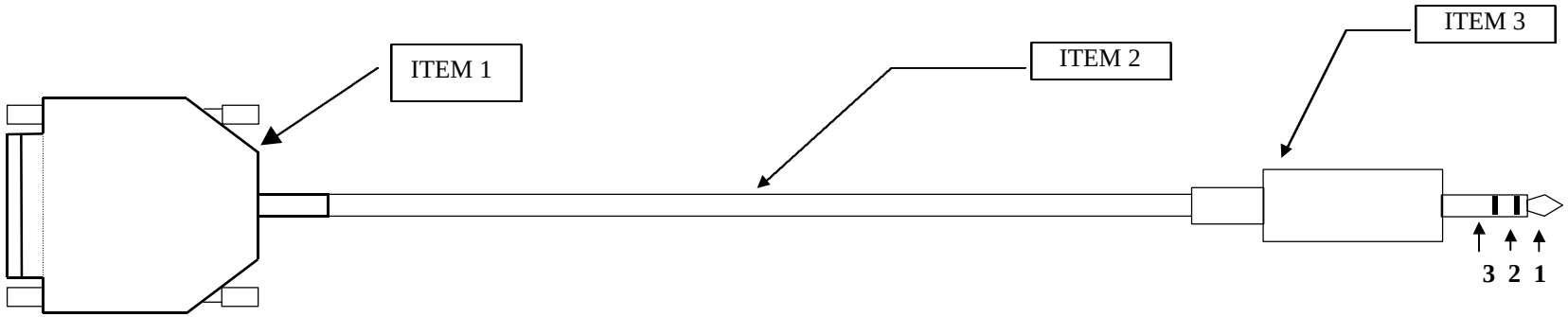
Table 9 : Applicability to the input / output PIN device used

Label	Description	Input Time	Output Time
T1	Track 0 strobe set-up time negative edge	-	250 µs
T2	Track 0 strobe set-up time positive edge	-	500 µs
T2-T1	Track 0 strobe pulse width	0.25 x T3	250 µs
T3	Track 0 bit time	1000 µs	1000 µs
T4	Track 2 strobe set-up time negative edge	-	125 µs
T5	Track 2 strobe set-up time positive edge	-	250 µs
T5-T4	Track 2 strobe width, OMRON = MAGTEK =	0.33 x T6 0.25 to 0.50 x T6	330 µs 250 µs
T6	Track 2 bit time	220 µS to 4mS	1000 µs
T7	Card Present hold time	10 mS to 30mS	10 mS
T8	Wiegand Pulse Width Time (=TPW)	10 µS to 100 µS	100 µS
T9	Wiegand Pulse Interval Time (=TPI)	200 µS to 20 mS	900 µS

Table 10 : Input and output timings

N.B. Unless stated otherwise all timings are nominal and subject to design tolerances and variances between the different type of PIN device available for use.

11.5 Cable connecting Verid+ to a PC



PARTS LIST

Item	Description
1	9 way Female D Type socket c/w solder buckets
2	2 core + screen cable.
3	3.5mm 3 pole Jack Plug - Rendar European type

WIRING SCHEDULE

9 Way D Type	Cable Core	Jack Plug
2	Clear	1
3	Blue	2
5	Screen	3

Note: This cable is available from TSSI as part of the *Verid Manager* kit.

Figure 15 : Cable to connect *Verid+* to a PC

11.6 Glossary

Verification	Comparison of a person's fingerprint against a template stored in memory. This is a one-to-one process.
Identification	Comparison of a person's fingerprint against all templates stored in memory to find the best match. This is a one-to-many process.
Template	A very brief "summary" of the fingerprint, containing information relevant to the matching algorithm. The full fingerprint image ***cannot*** be derived from the template.
Enrolment	The process every user and SuperUser must go through before they can use the system. When a new user is enrolled onto the system, a "template" of their finger is permanently stored in *Verid+*. The template is always associated with a PIN number which itself must be unique.
User	A user has no special privileges in *Verid+* they can only use the system to verify their fingerprint and cannot change mode, enrol new users or SuperUsers, or perform any other function.
SuperUser	A SuperUser can enrol new users and SuperUsers, can delete users (and SuperUsers, including him or her self!). A SuperUser can also make SuperUsers into normal users and visa versa. Typically a SuperUser may be someone chosen from the building security or front desk staff.
Supervisor Mode	A "Supervisor" can perform those tasks that may have to be performed on an infrequent basis, e.g. template transfer, setting and changing the unit's security level and allowing second templates. A "Supervisor" performs all functions via a PC connected to *Verid+* and need not be enrolled onto *Verid+*. The "Supervisor" has a password to allow the above tasks to be performed. Typically a Supervisor might be someone with responsibility for overall site management, or perhaps someone with responsibility for information systems support.
Configuration Mode	This mode should be used by an engineer who is installing *Verid+ units* on an end-user site. Connecting a PC to *Verid+*, and entering the "Configuration" password using e.g. *Verid Manager* enters "Configuration" mode. Once into configuration mode, examples of parameters that can be altered are: PIN input device, timeout and card present lines, card data format, erase entire database, and change the "Configuration" password.

12 Specification

Case Details:	
Height	190 mm
Width	120 mm
Depth	60 mm
Weight	0.5 Kg

Power Requirements:	
Input voltage (DC)	10 to 14 V DC
Current consumption	500 mA (max)

Temperature:	
Operation	0°C to 40°C
Storage	-10°C to 50°C
Humidity @ 40°C	10% to 80% (non-condensing)

Verid+ is designed so as to comply with UL294.

In order to meet the requirements of EN60950 (Safety) *Verid+* should be powered from an SELV supply.

Verid+ complies with the following EMC requirements:

Europe

EN55022 Emissions (class A) EN50130-4 Immunity (class A)

Warning: this is a "Class A" product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

North America

FCC rules CFR47 part 15 limit A

Verid+ has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is used in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference in which case the user will be required to correct the interference at his own expense.

12.1 Applicability (document versions)

See Table below. For other versions of *VERID+* Unit and *Verid Manager* Software some differences may apply. If in doubt please contact the TSSI Product Support line (see page 2) or your local TSSI approved supplier .

User Guide * Issue	*VERID+* Manager Version	*VERID+* Unit Version	Comments
5	4.0	VP1.00	Initial release (for Standalone units).
5	5.01	VP5.01	Verid Manager is recommended for use with VP5.01. Earlier versions will work but you will not be able to access new features or upgrade software beyond VP 5.01.

* *Verid Manager* User Guide OM/201

12.2 Changes to this manual

Revision /01 - Initial release for *VERID+* VP1.00

Revision /02 - Release for *VERID+* VP5.01

Enrolment scoring details added.

Information mode details added.

High Security mode details added.

Changes to Wiegand 2601 decoding added.

Various changes in wording made throughout manual to improve clarity of meaning.

Warning about the use of earlier versions of Verid Manager added.

13 Index

Access Control system
connecting VERID to the 14
Adding (Super)Users
via the LCD screen 18
via the RS232 port 26
Algorithm ..... See Technical details
CardPresent ..... See TimeOut & Card Present
Changes - new features in OM202/03 46
Cleaning 38
Compatibility with earlier versions of Verid 39
Configuration details
factory default settings 6
Configuration Mode
database, erase or empty the 19
LCD text, changing the 19
options available in 19
overview 17
PIN device - reconfiguring 19
settings changeable from 19
using VERID Manager 19
Connections - wiring details 17
Contact details 2
Database management ..... See VERID Manager
Deleting users
via the RS232 port 26
e-mail address 2
Empty database ..... See VERID Manager
Enrollment of
the 1st SuperUser or User 23
the 2nd and subsequent users 24
Error – PIN output signals 16
FAQ / fault finding 37
Getting started **5**
using VERID for 1st time 21
Glossary 44
Installation
fixing details 8
guidelines 7
input power requirements 9
output power from VERID 9
Introduction **6**
Keypad
choosing a new PIN 23
compatible formats 13
output format 14
LCD
changing the default messages 20
type used in VERID 20
LED ..... See also Supervisor Mode
default settings 14
external control of the 14
power-up sequence 9
Maintenance & replacement parts 38
Network
add / update a user 30
adding a new unit 30
adding units to a 33
auto-configure 32
Auto-configure 30
changing user properties 30
database synchronisation 30
deleting users 30
getting started 30
installing 32
LED power-up sequence 30
LEDs after power-up 31
overview 28
setting addresses 33
technical guidelines 33
VERID Manager and 33
wiring details 28
wiring diagram 28
output power ..... *See* "Installation"
PC to VERID RS232 lead 43
PIN device
checking operation 13
connections, an overview 9
keypad device - connections 12, 13
proximity device - connections 11
track 2 device - connections 9
Watermark device - connections 12
Wiegand (intelligent) - connections 11
Wiegand device - connections 10
PIN formats
error signals for each format 16
intelligent Wiegand 11, 12
keypad 13
maximum length (track 2) 10
track 2 10
Watermark 12
Wiegand 10
power ..... See "Installation"
RS485 ..... *See* Network
Safety 8, 9, 37, 45
Security levels 21
Global 21
users 21
VERID 21
Specifications
electrical 45
FCC 45
power 45
temperature 45
SuperUser Mode
entering the 17
how to enter the 21
overview 17
Supervisor Mode
available options 18
change password 18
entering the 17
LED control 18
optional settings 18
overview 17

security level 18
start enrolment 18
start transparent 18
start verification 18
Supervisor Mode and VERID Manager 18
Support, phone / fax / e-mail / web 2
Technical details 40
matching algorithm 40
timing diagram (input & output) 41
Templates
creating a 35
encoding onto track 3 36
generating, in track 3 format 35
magnetic card track format 35
managing 26
methods of transferring 26
storing on a mag card 35
storing on track 3 35
track 3 data format 36
TimeOut & CardPresent
factory defaults 14
output 14
using 14
Tips for finger placement 22
Track 3
data format, timing and content 35
Troubleshooting 37
Update template
via the LCD screen 18
Users - maximum capacity 40
VERID Manager
change configuration using 17
empty database 27
managing template database 27
VERID to PC RS232 lead 43
Warranty 2
Web address 2
Wiegand ..... *See* PIN formats - Wiegand

TSSI
Rutland House
Hargreaves Road
Groundwell Industrial Estate
Swindon
Wiltshire SN25 5AZ
U.K.

Tel: +44 1793 747700
Fax: +44 1793 747701
Email: *Verid*+@TSSI.co.uk
Web: http://www.TSSI.co.uk